AI-Powered Blockchain - A Decentralized Secure Multiparty Computation Protocol for IoV

[1]Gunasekaran Raja, [2]Yelisetty Manaswini, [3]Gaayathri Devi Vivekanandan, [4]Harish Sampath,
[5]Kapal Dev, [6]Ali Kashif Bashir
[1,2,3,4]Department of Computer Technology, Anna University, Chennai, India,
[5]CONNECT Centre, Trinity College Dublin, Ireland,
[6]Department of Computing and Mathematics, Manchester Metropolitan University, UK,
[1]dr.r.gunasekaran@ieee.org, [2]manaswini1511@gmail.com, [3]gaayathri1704@gmail.com, [4]harish28399@gmail.com,
[5]kdev@tcd.ie, [6]dr.alikashif.b@ieee.org

***Abstract*—The rapid advancements in autonomous technologies have paved way for vehicular networks. In particular, Vehicular Ad-hoc Network (VANET) forms the basis of the future of Intelligent Transportation System (ITS). ITS represents the communication among vehicles by acquiring and sharing the data. Though congestion control is enhanced by Internet of Vehicles (IoV), there are various security criteria where entire communication can lead to many security and privacy challenges. A blockchain can be deployed to provide the IoV devices with the necessary authentication and security feature for the transfer of data. Blockchain based IoV mechanism eliminates the single source of failure and remains secure at base despite having strong security, the higher level layers and applications are susceptible to attacks. Artificial Intelligence (AI) has the potential to overcome several vulnerabilities of current blockchain technology. In this paper, we propose an AI-Powered Blockchain which provides auto coding feature for the smart contracts making it an intelligent contract. Moreover, it speeds up the transaction verification and optimises energy consumption. The results show that intelligent contracts provide higher security compared to smart contracts considering range of different scenarios.**

***Index Terms*—Blockchain, Artificial Intelligence, Smart contract, Internet of Vehicles, Vehicular Network**

I. Introduction

Modern lifestyle has led to an extensive usage of private transport vehicles that saves a lot of time and gives owners the required privacy. In this era, there is a need for future vehicles to be fully autonomous, more comfortable and greener. Since the impact of technology on our lives keep increasing with time, VANET has evolved to meet the growing demand [8]. A large range of VANET applications including road safety, car services related to manufacturing units, optimization of vehicular traffic and passenger infotainment can be enhanced using wireless communication.

The development of Internet of Vehicles (IoV) technology leads to a large number of vehicular nodes accessing the network. This centralized system can handle large amount of traffic generated from vehicular interaction. As the traffic load increases on the traditional centralized server, it faces significant challenges [1]. The whole system may crash if the central server fails, leading to huge disruption. So, there is a need to consider decentralized management and distributed storage as the future technology. This is the current progression of technology towards the next generation of IoV [8]. The decentralized technology demands high security for the exchange of data and communication between vehicles.

As a solution to the issue of secure sharing of information among vehicles, blockchain can be used to solve the problem of secure information exchange between vehicles [10]. Unlike the traditional client- server model, blockchain supports peer-to-peer (P2P) communication. The mining nodes of the blockchain have a ledger which holds all of the transactions that took place and contains chained blocks. Therefore, a secure log is created with timestamped records that can never be altered because of proof of work (PoW). Blockchain solves the problem of trusted interactions using decentralized approach and provides the necessary authentication and authorization to IoV devices. It is also a cost effective approach as it reduces the deployment, performance overhead and operational costs of IoV.

The smart contract is the heart of the blockchain, where the rules regarding the interactions are presented [13]. It digitally facilitates, verifies and enforces the performance of the contract. Using smart contracts, the need for the third parties to validate the transaction is eliminated. All the users of the blockchain network can view the smart contract as this enables more people to check that the code is good but may lead to large security holes and attacks. These attacks include escalation of funds if proper care is not taken into consideration to create the smart contract rules. In consequence, the proposed decentralized AI-Powered blockchain is designed which is basically a combination of AI and blockchain.

The AI-Powered blockchain is capable of processing the stored data and intelligently enables decision making which predicts the nature of the interaction and also the resources it utilizes. The decision outcomes are validated by the trusted mining nodes of blockchain. Integration AI and blockchain has benefits such as data security enhancement and improving trust in the decisions made by AI [17]. In this paper, the auto coding feature for the smart contract is provided by the integration

of AI with blockchain, thus making the smart contract an intelligent contract. These intelligent contracts make use of Natural Language Processing (NLP) to auto code and use the previous data to make smart decisions. The proposed AI-Powered Blockchain ensures that the implementation of a smart contract is free of bugs and secure against attacks. The potential vulnerabilities are ruled out as they are automatically handled by proposed intelligent contract.

II. Related Work

VANET is a subset of larger set of vehicular networks called Mobile Ad-hoc networks (MANET). Vehicles communicate with each other supporting highly dynamic networking topology, but this communication whilst enhancing the passenger's safety and comfort is vulnerable to many attacks [1].

For dynamic security association, security protocols are proposed, which provides high robustness and efficient key management systems [2,3]. Since the vehicles interact amongst themselves through internet protocols, the Internet of Things (IoT) network is formed. The 5G technology has emerged providing data speeds a hundred times faster than 4G and provides a better bandwidth. It is combined with Software-Defined Network (SDN) architecture for information gathering at global level [4,5].

Blockchain is a distributed, decentralized value-exchange protocol which records transactions across a huge network and prevents alteration of any record as it requires changes to subsequent blocks. The entire working mechanism of blockchain makes it more adaptable to IoT . There are a lot of benefits in combining the blockchain with IoT such as efficient fraud management and supply chain management [6].

Smart cities are developed as a result of the enhanced technology advancement by the blockchain. A smart city is an architectural setup that overcomes the challenges of urbanization by combining new technologies [7]. This builds an intelligent transportation system in the smart city which is secure and autonomous. Security is ensured by preventing data forgery and personal information breach by making use of blockchain technology for vehicular networking [8]. Social networks require highest level of privacy protection to prevent information leak to malicious users [9].

Various security services like authentication, integrity assurance and confidentiality are automated using the blockchain [10]. This resolves the challenges of the state of art techniques used in the current applications. In [11], a trusted connection is established between the interacting entities using the universal data object identifier platform enabling secure digital object management.

In order to make the entire system more effective, the user should be aware of the blockchain consensus algorithms being used and also the blockchain taxonomy. The technical challenges as well as the recent advancements in tackling the challenges should be known. A comprehensive survey and review on blockchain is conducted to analyze and adapt the technology based on the specific needs of the application in [12]. Blockchain interactions take place through smart contracts which is decentralized trusted shared code [13]. The smart contracts enforce rules based on which interactions take place. The execution of smart contracts and their environments are also vulnerable to attacks. AI is used to overcome these challenges which boosts the efficiency of the system by many folds.

AI gives the opportunity to tackle blockchain tasks in a very intelligent and efficient way [14]. Integrating AI and blockchain benefits the entire system by making use of low computational power and creates diverse datasets for further efficient processing. Transportation system has been embedded with intelligence to meet the requirement of easy movement and interaction among vehicles [15,16]. A more trusted cyber space is created by this powerful combination that ensures security by introducing many intelligent rules [17]. These rules are automatically generated by AI using enormous amount of data retrieved from the blockchain.

III. Proposed Work

In this section, we propose an AI-Powered blockchain which solves the problem of traditional issues in the existing system to create a safe and secure VANET framework. The proposed system leverages the power of AI and a robust blockchain network to protect assets from security breaches and attackers. This AI-Powered Blockchain system is applicable to both static and dynamic VANET environment.

A. Blockchain Based IoV Network

In IoV network, safe driving and better service quality is achieved by sharing data among the vehicles in a lane. The traditional centralized management structure in IoV requires large data and information storage. This requirement puts forth many challenges and real-time responses that cannot be efficiently dealt with the existing architecture. In addition, data manipulation of personal information uploaded to the infrastructure can be a hindrance for the future development of IoV. Thus, blockchain technology makes the system more secure, scalable and fault tolerant.

Blockchain addresses many failures and scalability bottlenecks. As the number of vehicles increase, there is an equivalent increase in the number of interactions in the IoV network. As a consequence, there is a need for a P2P network instead of the traditional client-server model which is fulfilled by blockchain technology. Currently, the integration of blockchain with IoV is in the limelight because of the trusted characteristics of blockchain. Though the entire process is still complicated, it provides various features like decentralized distributed processing, anonymity, trusted authentication and verification required for the IoV network to succeed.

In the VANET environment, Road Side Unit (RSU) is deployed with blockchain as the controller. RSU helps in storing the information of the passing vehicles in the blockchain. Since the RSU, petrol pumps, toll gates etc., are static, they act as miner nodes in blockchain. Each vehicle in the blockchain network is connected to nearby peer vehicles as depicted in Fig. 1. Data stored in toll gates, petrol pumps, RSU is also used

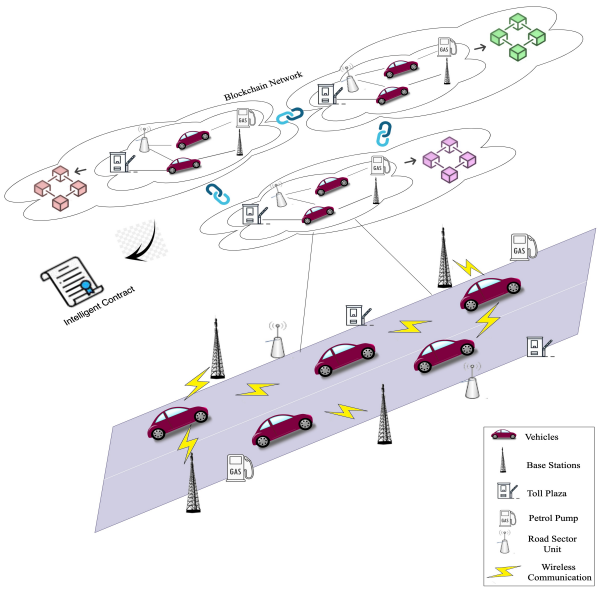

Fig. 1. Blockchain-based IoV

by vehicles for easier communication with the infrastructure. All the vehicles are registered independently in the blockchain network. When the vehicles register with the help of RSU, ethereum blockchain transactions take place. A small amount of fee is charged to register them into the network. Once registered, the vehicle will broadcast an event message such as traffic jam, road conditions, shortest path, accident, etc. to neighbouring vehicles. Miner nodes in the blockchain network validate the authenticity of the message before propagating it to the peer vehicles. The vehicle will broadcast the message to the peers, if the event message is validated to be true. Thus, the tamper proof nature of the blockchain stores and manages the event messages. Every information recorded on the blockchain becomes a verified transaction, once it is validated and signed by the neighbouring nodes. Various cryptographic algorithms are employed by the blockchain which helps in the generation of the hash key. Each block is sequentially ordered based on their hash values. The broadcasted message gets updated in each vehicle's block in the blockchain network. There are millions of vehicles and if each region forms a separate blockchain, there will be a significant decrease in scalability issues.

B. AI-Powered Blockchain

The current problem with the blockchain technology is, it can never create mass adoption because of its complexity. AI and blockchain could be a splendid combination because of highly sensitive and large amount of data is stored in blockchain which is to be supplied for the AI engine to make statistical and analytical decisions. Blockchain provides the data to be processed by AI for predictive analysis and also improves the performance of the system on a great scale. The AI-Powered Blockchain envisages the following key points:

- Blockchain creates a strong base layer but the higher end application layers have potential vulnerabilities which may get exploited by hackers causes irreparable loss. AI tremendously improves the deployment of blockchain application by predicting possible system breaches and enhances the total security of the system.
- Every node in the blockchain has a distributed ledger that has all the decisions made by the particular node. This ledger data becomes available to AI for analysis and processing. The integrity of data recorded for examination is ensured because blockchain is tamper resistant.
- Blockchain's smart contract code can be viewed by all the nodes taking part in the transaction. Therefore, it is vulnerable to attacks and can be exploited by hackers. These attacks can be prevented using AI which can predict the possible vulnerabilities and introduce new intelligent rules, improving the nature of the smart contract.
- By adopting intelligent contracts, in VANET environment when there is an increase in number of mining nodes, compared to other existing approaches, our proposed AI-Powered blockchain decreases the processing time by 25%.
- Transactions can be verified faster, energy consumption can be optimized and smarter smart contracts are used which benefits the blockchain.

1) Ethereum setup: AI-Powered Blockchain is modelled on Ethereum, an open source platform for distributed applications. It is a decentralized account-based blockchain implementation. There are two types of accounts namely Externally Owned Account (EAO) and contract account. The EAO triggers the contract account. Contract account is the byte code and it incurs the cost for its valuable computation and storage resources of the network. Ethereum allows people to safely communicate in a peer-to-peer fashion. A runtime environment is created by Node Package Manager (NPM). Ethereum transaction is demonstrated using the Ganache simulator. The ganache is set up with user accounts loaded with fake ether. Ether is the digital currency used in the blockchain transactions.

2) AI-Powered Blockchain dependencies: The ethereum environment is set up and various dependencies necessary to implement the blockchain are installed. NPM is the basic need to install all other dependencies for the Blockchain-based IoV environment. Secondly, the truffle framework that has a suite of tools to write smart contracts is incorporated. The client side application is developed using this truffle framework and also allows the user to test and deploy the smart contracts. Smart contracts are developed using Solidity, an object-oriented, high-level programming language. The next dependency is Ganache, a local blockchain setup, used in the creation of decentralized applications and useful for testing the desktop applications. To make use of the ethereum blockchain setup, Metamask extension of google chrome is enabled. It is used to interact with the smart contract and also runs the decentralized ethereum application in the browser by providing a secure vault.

3) Intelligent Contracts: Smart contract is the vital component of the blockchain environment but they are not smart enough as they may come with several vulnerabilities. The smart contract code consists of rules that are executed when certain conditions are met. Since the smart contract code is public, any malicious intruder can go through each line of the code patiently in search of loopholes. Once the loopholes or the technical flaws are found out, they can be taken advantage of and exploited the whole network such that funds can be malevolently released or transferred. The attackers can also attack once they know how the events take place in the VANET environment. To enhance the smart contract and make it intelligent, we integrate AI with blockchain with the help of dependencies.

In our proposed AI-Powered Blockchain model, the decentralized ethereum application uses an autocoded intelligent contract which tremendously improves its efficiency. We used NLP to autocode the smart contract and Naive Bayes classifier to predict the tag for the each user request as illustrated in algorithm 1. For making intelligent decisions for each request, the contracts gets influenced by historical data and prototyping concepts. Thus, for a particular application, each vehicular user needs to specify the features to be included in their respective block in the blockchain network. The coding of the contract is then automatically handled by AI techniques. The proposed system makes the smart contract intelligent by adopting the text classification and autocoding procedure as illustrated in the below algorithms.

$$P(C_n|V) = \frac{P(V|C_n)P(C_n)}{P(V)} \tag{1}$$

where, V = $(v_1, v_2, ..., v_n)$ is the feature vector,
$P(C_n|V)$ is the posterior probability,
$P(V|C_n)$ is the likelihood,
$P(C_n)$ is the prior probability of class,
$P(V)$ is the prior probability of the predictor

All the features received as input from the user are not dependent on each other. There exists conditional independence among the set of features. Since Naive Bayes algorithm also works with the naive assumption of conditional independence, it is the most suitable for generation of the contract.

The probability of a Vehicular_Request (Veh_Req) belonging to a class cl is calculated. The maximum likelihood estimate is then found out to estimate the parameters. In algorithm 1, the vocabulary for the given vehicular user request is extracted as a set of tokens $(t_1, t_2, \ldots, t_n)$ and used for classification as depicted in Fig. 2. N is the total count of Veh_Reqs. N_{cl} is the number of Veh_Reqs belonging to a particular class cl. The prior probability for each class cl is calculated as follows:

$$prior[cl] = \frac{N_{cl}}{N} \tag{2}$$

$text_{cl}$ is the text concatenated from all the Veh_Reqs belonging to that class cl. T_{ct} stores the count of number of times the vehicular user input information t is appearing in the $text_{cl}$. For each class, the conditional probability is calculated for all the tokens as mentioned in equation 3.

$$condprob[t][cl] = \frac{T_{ct} + 1}{\sum_{t'} T_{ct'} + 1} \tag{3}$$

Algorithm 1 Classification of text

Input: Vocabulary for the vehicular user request
Output: Probabilities of the output classes

procedure TRAIN MULTINOMIAL (C, VEH_REQ)
  Voc ← *VocabularyExtraction(Veh_Req)*
  $N \leftarrow$ *Veh_ReqCount(Veh_Req)*
  for $cl \in \mathcal{C}$ **do**
    $N_{cl} \leftarrow$ *ClassWise_Veh_Reqs_Count(Veh_Req,cl)*
    $prior[cl] \leftarrow N_{cl}/N$
    $text_{cl} \leftarrow$ *TextConactenationOfAllVeh_ReqsInClass*
    for $t \in \mathcal{V}oc$ **do**
      $T_{ct} \leftarrow$ *TokensCountOfTerm*$(text_{cl}, t)$
      for $t \in \mathcal{V}oc$ **do**
        $condprob[t][cl] \leftarrow T_{ct} + 1/\sum_{t'} T_{ct'} + 1$
  return $Voc, prior, condprob$

Algorithm 2 Prediction of the output class

Input: Calculated probabilities
Output: Classified text is obtained

procedure APPLY MULTINOMIAL (C, VOC, PRIOR, CONDPROB, VEH_REQ)
  $P \leftarrow TokensExtraction(Voc, Veh\_Req)$
  for $cl \in \mathcal{C}$ **do**
    $result[cl] \leftarrow logprior[cl]$
    for $t \in \mathcal{V}oc$ **do**
      $result[cl] \leftarrow result[cl] + logcondprob[t][cl]$
  return $argmax_{cl \in C}\, result[c]$

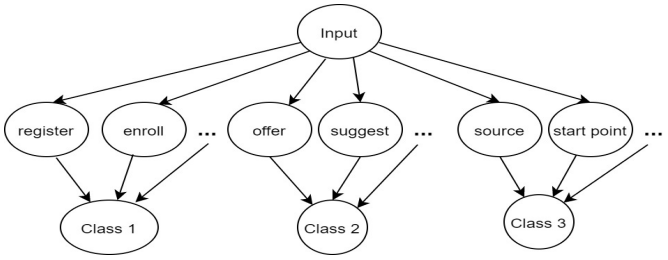

Fig. 2. Vehicular Request classification

To predict the class of the Veh_Req, tokens are first extracted as shown in algorithm 2. For each class, the result variable stores the log of prior probability. The log of conditional probability of each token is then added to the class prior probability as a final result. The class with maximum score is chosen as the predicted class to which the Veh_Req belongs.

Once the Veh_Req is classified, we use the Bayesian network to autocode the contract, making it an intelligent

contract. Bayesian networks is used for probabilistic queries as it represents an entire model comprising of conditional dependencies via a directed acyclic graph. The joint probability distribution over all the variables of a Bayesian network model, P(V), is the product of the probability distributions over each of the nodes conditional on their parents as shown in equation 4. To calculate $P(E = e)$, we need to sum over all $P(V \backslash E, E = e)$ as shown below:

$$P(V) = \prod_{i=1}^{n} P(Vi|Pa(Vi)) \tag{4}$$

$$P(E = e) = \sum_{V \backslash E} P(V \backslash E, E = e) \tag{5}$$

where, E is the evidence variable,
$Pa(V)$ denotes the parent of node V

The parameter class id (c_id) is the predicted output class from algorithm 2. c_id represents the type of Veh_Req and the rules that have to be framed. The rules pertaining only to that class are involved in the generation of intelligent contract.

Initially, the various events in VANET environment are arranged in topological order. For every event, initialize the following variables: $Pr^0(X \backslash E)$ represents the importance function, t represents the time interval and n represents the number of samples. Each solution s_i is generated within t seconds and appended to the set of solutions S. The score function calculates the score of every solution and then makes a corresponding entry in the score array. The score is calculated based on parameters like time complexity, space complexity, ordering of the rules, etc. We normalize the score array for every event and the one with the maximum score is chosen as the final solution as illustrated in algorithm 3. Thus, the proposed AI-Powered Blockchain system makes the smart contract intelligent by adopting the autocoding procedure and improves the overall security in VANET environment.

Algorithm 3 Autocoding smart contract

Input: Classified text is given as input
Output: Autocoded smart contract

procedure AUTOCODE(c_{id})
  Topological sorting of the events
  Initialize $\text{Pr}^0(X \backslash \text{E})$, t, n, and the score
  $c \leftarrow 0, S \leftarrow \emptyset$
  for j $\leftarrow$ 1 to n **do**
    if j mod t == 0 **then**
      $c \leftarrow c + 1$
      Update $\text{Pr}^0(X \backslash \text{E})$ based on S
    end if
    $s_i \leftarrow$ sample generated in accordance to $\text{Pr}^c(X \backslash \text{E})$
    $S \leftarrow S \cup s_i$
    Calculate the score for every solution (s_i)
  Normalize the score arrays for every event
  return max(S)

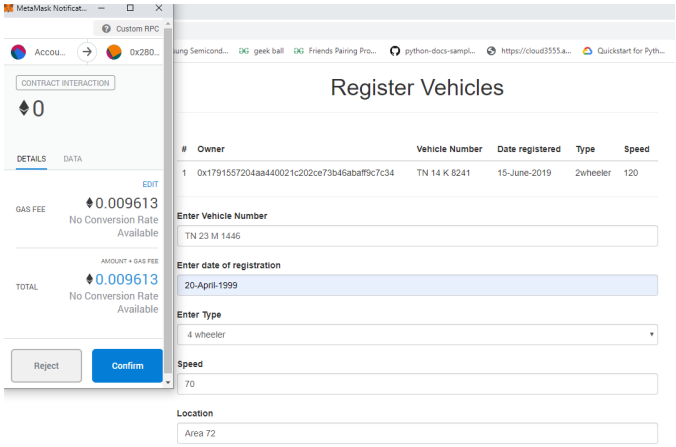

Fig. 3. Ethereum transaction

IV. Performance Analysis

In this section, we compared the performance of our AI-Powered Blockchain system with the existing smart contract in blockchain. The comparison is made to depict the security with respect to various scenarios. The vulnerabilities in smart contracts have led to major attacks causing a lot of loss to the organizations deploying blockchain. With an advancement of technology, the attackers have also geared up and they are exploiting the loopholes over the platform compromising the security in networks. AI makes the system learn through out its lifetime and improves the results taking the network security to peaks. The auto coding feature of smart contracts using AI overcomes many of the challenges faced in the current system paving way to more efficient, reliable and secure system.

For every vehicle being registered, an ethereum blockchain transaction takes place as shown in Fig. 3. The transaction window consists of the amount being charged for that transaction. This amount is also known as the gas fee in the blockchain world. Gas fee is charged only for the transactions that require writing into the blockchain. Amount is not deducted for the transactions that require only fetching the vehicular user data.

The smart contract and intelligent contract generated for fetching details of a vehicle is shown in Fig. 4. The proposed intelligent contract is generated uniquely and dynamically from the given user request. The code is constructed by classifying the input using classifier algorithm. In order to select the finest classifier algorithm, comparison is made based on performance parameters namely F-measure, accuracy and area under curve (AUC). Naive Bayes classifier has approximately 20% increase in the performance parameters compared to k-nearest neighbors (KNN) algorithm and Decision Tree as shown in Fig. 5. Hence, Naive Bayes classifier is used to predict correct class to which the given Veh_Req belongs, and the contract will be autocoded accordingly.

From Fig. 6, the security for various blockchain scenarios such as money transfer, fraud deterrent, creating transparency, syndicated lending, anti-money laundering is tested. It can be seen that the percentage increase in security is comparatively

```
Smart Contract
function fetch_details (string memory _vehicleId,string memory asker) public {
    require(register[_vehicleId]);  // check if the vehicle is registered
    if( asker == owner[_vehicleId])
    {
      for (uint i=0; i<vehiclesCount; i++)
      {
        if( vehicles[i].vehicleId == _vehicleId)
          return vehicles[i];
      }
    }
  }
}
```

```
Intelligent Contract
function fetch_details (string memory _vehicleId,string memory asker) public {
    require(valid_format[_vehicleId]); //check if it is valid vehicle
    require(register[_vehicleId]);
    if( asker == owner[_vehicleId])
    {
      return vehicle_details[_vehicleId];
    }
    else
      return false;
    }
}
```

Fig. 4. Smart contract Vs Intelligent contract

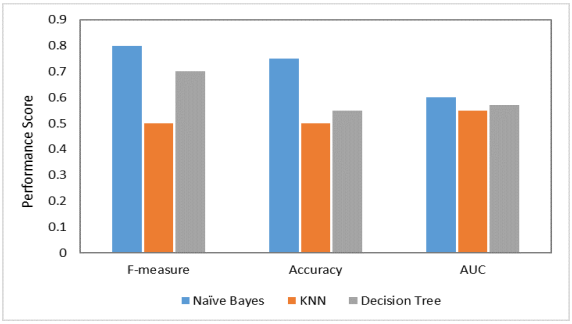

Fig. 5. Classifiers comparison

high when intelligent contract is used in the place of smart contract. Hence, the proposed intelligent contract of AI-Powered Blockchain is highly secure than smart contracts.

V. Conclusion

In this paper, we investigate how the AI-powered Blockchain technology can be applied in IoV applications to overcome the security challenges. Our proposed scheme creates more efficient and reliable system with the combination of AI with blockchain. The auto coding feature of intelligent contract is implemented using Bayesian networks. This creates a better blockchain network and more security rules are framed through AI-powered Blockchain during the lifetime of the system. The future is towards more secure intelligent systems and our paper contributes to the field of vehicular networks using AI.

Acknowledgement

This Publication is an outcome of the R&D work undertaken in the project under the Visvesvaraya PhD Scheme of Ministry of Electronics Information Technology, Government of India, being implemented by Digital India Corporation (formerly Media Lab Asia).

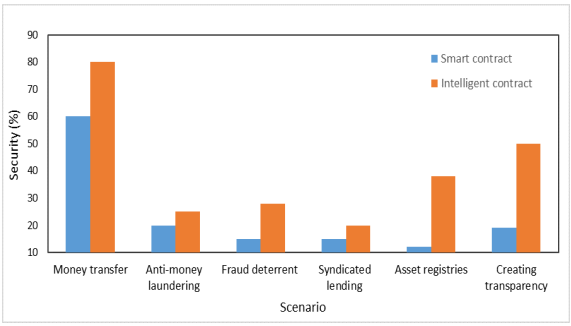

Fig. 6. Smart contract Vs Intelligent contract

References

[1] H.P. Dai Nguyen and R. Zoltán, "The Current Security Challenges of Vehicle Communication in the Future Transportation System," in IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, pp. 0161-0166, 2018.

[2] R. Arul, G. Raja, A. O. Almagrabi, M. S. Alkatheiri, S. H. Chauhdary and A. K. Bashir, "A Quantum Safe Key Hierarchy and Dynamic Security Association for LTE/SAE in 5G Scenario," in IEEE Transactions on Industrial Informatics, July 2019.

[3] R. Arul, G. Raja, A. K. Bashir, J. Chaudry and A. Ali, "A Console GRID Leveraged Authentication and Key Agreement Mechanism for LTE/SAE," in IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 2677-2689, June 2018.

[4] L. Xie, Y. Ding, H. Yang and X. Wang, "Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs," in IEEE Access, vol. 7, pp. 56656-56666, 2019.

[5] G. Raja, A. Ganapathisubramaniyan, S. Anbalagan, S. B. M Bhaskaran, K. Raja and A. K. Bashir, "Intelligent Reward based Data Offloading in Next Generation Vehicular Networks," in IEEE Internet of Things Journal, DOI:10.1109/JIOT.2020.2974631, 2020

[6] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[7] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-VN: A distributed blockchain based vehicular network architecture in smart city, " in J. Inf. Process. Syst., vol. 13, no. 1, pp. 184–195, Mar. 2017.

[8] T. Jiang, H. Fang and H. Wang, "Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4640-4649, Jun. 2019.

[9] R. Yu et al., "Authentication With Block-Chain Algorithm and Text Encryption Protocol in Calculation of Social Network," in IEEE Access, vol. 5, pp. 24944-24951, 2017.

[10] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," in IEEE Communication Surveys Tutorials, 2018.

[11] H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu and J. Xing, "Hyperconnected Network: A Decentralized Trusted Computing and Networking Paradigm," in IEEE Network, vol.32, no. 1, pp. 112-117, Jan.-Feb. 2018.

[12] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," in IEEE Access, vol. 6, pp. 32979-33001, 2018.

[13] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F. Y. Wang, "An overview of smart contract: architecture, applications, and future trends," in IEEE Intelligent Vehicles Symposium (IV), pp. 108–113, 2018.

[14] K. Salah, M. H. U. Rehman, N. Nizamuddin and A.Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges, " in IEEE Access, vol. 7, pp. 10127-10149, 2019.

[15] S. Saharan, S. Bawa and N. Kumar, "Dynamic pricing techniques for Intelligent Transportation System in smart cities: A systematic review," in Computer Communications, vol. 150, pp. 603-625, 2020

[16] A. Miglani and N. Kumar, "Deep learning models for traffic flow prediction in autonomous vehicles: A review, solutions, and challenges," in Vehicular Communications, vol. 20, 2019.

[17] K. Wang, J. Dong, Y. Wang and H. Yin, "Securing Data With Blockchain and AI," in IEEE Access, vol. 7, pp. 77981-77989, 2019.