ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 11, November 2018

Prevention of Odometer Fraud Using Blockchain Technology

[1] Deepanshu Kapoor, [2] Shubham Gupta, [3]Anushka Gupta, [4]Dishant Grover, [5]Silica Kole
[1][2][3][4][5] Bharati Vidyapeeth College of Engineering, New Delhi

Abstract: The used automobile industry is an ever expanding disarray. With this pace of expansion, the industry is also subject to a few vulnerabilities. The industry is based around only a few factors including official documents regarding the manufacturing date, sale deed, service record and the mileage of the car. Documents are protected by the government departments while the mileage is a variable under the tertiary influence. Odometer readings area unit the proof of the gap a automotive has traveled. This helps the customer to understand regarding the condition of the automotive. This is a fraudulent activity, scamming the buyer of his right to transparency and truth, that resulting in distrust between the customer and also the trafficker. The problem of trust in the digital world is being solved by using blockchain. We are just putting in an effort to provide trust to the people using the digital mechanism in the used automobile industry.

Keywords: API (Application Interface), OBD (On-Board Diagnostics), PID (Parameter IDs)

1. INTRODUCTION

The used industry in India may be a large market with a turnover of over $50 billion. An large vary of shoppers area unit inclined to used cars because of their affordability and improved after-sales services. Being either digital or analog in nature, car's odometer is easy to be meddled with. When a customer purchases a second-hand car, the first thing that catches his attention, besides the vehicle's condition, is 'how many miles the car has clocked?' The fewer the miles, the higher is the price. So, Odometer tampering has become a commonplace fraudulent practice to make the car seem a lot engaging to prospective consumers and to effectively steal cash by charging a lot for the car than it's actual price Associate in Nursing odometer mechanic may simply replace the chip that stores the milometer reading by another one with the specified reading and hence, increase its market price and dupes the consumer. Tampering in a digital odometer can be done just with the help of a laptop and appropriate software. Moreover, with little evidence of this kind of tampering, it is nearly impossible for an average customer to detect this kind of fraud. Not just in used cars, odometer fraud is a common practice by taxi drivers who get paid for fuel per kilometer basis. The speedometer outlets will move an odometer back, forward and alter the activity too. meter change of state could be acriminal act, and it ends up in severe charges and severe penalties if guilty. in step with the National route Traffic Safety administration over 450,000 vehicles with false meter reading are sold once a year and prices automobile patrons over $1 billion. To counteract the issue of the ingenuity of the odometer reading due to its mutable nature, a blockchain model can be implemented to store the number of kilometers a car has driven with its various other parameters in an immutable chain of data blocks. This data block would have the hash, i.e., a signature of the particular car identified with its chassis number as a unique identifier. Blockchains are distributed ledgers, i.e., a decentralized database. Blockchain is a sequence of blocks, with the first block named Genesis Block. Due to the computationally intensive nature of verification of a blockchain, a blockchain is virtually immutable. The question is how to solve data tampering attacks on the chain; the solution is proof of work. As this can be a suburbanized peer to see server, thence there's no would like for a middleman. It is a transparent system hence any buyer, and a government official shall have an access to the required details about the car remotely. Access can be based on the authority of the person accessing it; hence a digital signature provides the details of permissions that are allocated. Furthermore, by putting in contrast the hash of the data block, the authenticity can be determined. The readings of the odometer and various other parameters would be periodically stored in a blockchain. The chassis number of the car would uniquely identify this block of data. The new block would be verified given a parameter that it does not decrease and other restrictions.

II. RELATED WORK

Blockchain technology was first introduced for the digital currency Bitcoin, however, later on technical communities started looking for other areas where it can

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 11, November 2018

be used. Blockchain consists of information which is stored on a chain of computers. The records of the information are really public, simply verifiable and can't be corrupted as dynamical knowledge on the blockchain would mean using a massive amount of computing power to override the whole network. Hence, the blockchain technology has varied applications. Crosby et al. mentioned that blockchain creates a distributed record or public ledger of transactions which are shared among all involved parties. Every dealing at intervals the general public ledger is verified by agreement of a majority of the participants at intervals the blockchain system. The data once entered cannot be deleted. The whole record of transactions is certain and verifiable. Three points are necessary for blockchain technology - Validate Entries, Safeguard Entries and to Preserve Historic Record [14]. Thakur et al. wrote that Blockchain 1.0 consists of digital currency applications, the blockchain 2.0 considers Smart contracts whereas the blockchain 3.0 considers a scenario beyond currency and economics. here are four types of blockchains- Permissionless, Permissioned, Public and private. Their paper classified various blockchain primarily based system configurations against multiple parameters like performance, price potency, and adaptability. Various dimensions of a blockchain system like blockchain configuration, computation, storage, a degree of decentralization are thought of in arising with the taxonomy. They also listed possible future applications in various fields such as digital identity provisioning, voting, commodity trading, reputation management, education, private data storage, insurance, smart cities, healthcare, and taxation[7]. Lansiti et al. explained that blockchain will completely transform business and government in a few years. This is as a result of blockchain could be a foundational technology that has potential to develop new economic and social structures. Financial services companies are already adopting the blockchain technology, but manufacturing companies have not started it yet [1]. Eyal et al. wrote that scalability barrier is a common issue faced by blockchain. The time complexity at which these systems can process transactions is constrained by the choice of two parameters namely, block size and block interval. Throughput is magnified by larger block sizes however the larger blocks take longer time to propagate within the network. Reducing the block interval leads to instability and the blockchain has to be reorganized. However, it reduces latency.[8]. Zyskind et al. used both blockchain and off-blockchain storage and constructed a data management platform. Blockchains may become a significant resource in trusted-computing, information transparency, and auditability. every user has complete transparency over what information is being collected regarding them and the way they're accessed. Mobile applications need the user to grant a group of permissions upon sign-up. Normally these permissions once granted are for indefinite period. But they proposed a system in which a user can alter the permissions anytime and revoke access to information. This mechanism would help to improve the existing permissions dialog in mobile applications. The UI tends to remain same but the access control policies will be securely stored on a blockchain. Service profiles were stored on a blockchain and their identity was verified.[2]. Dorri et al. presented a trailblazing vision on making interacting vehicles more secure using blockchain. Instead of centralized data, they used blockchain, so that the communication can be preserved without compromising the security. Lack of privacy can be reduced by using blockchain as the need for more personalized content is on a distributive encrypted network instead of sharing data with other vehicles without a secure layer around it. Blockchain improves security over many layers of applications like Insurance, Smart Car Charging [3]. In a similar work, Chanson et al. also presented a model for prevention of odometer fraud using blockchain. It records mileage and GPS information of cars and secures that on the blockchain, that powerfully prevents odometer fraud. A dongle was used to obtain odometer and GPS readings from the car and then this data was sent to an application where timestamp and a nonce were added to it. he dataset was then hashed and written on a public Ethereum blockchain. The transaction is signed regionally with the non-public key of the user and solely then it's sent to an Ethereum consumer within the cloud. The whole raw dataset is saved during a cloud information once secret writing. A smartphone app provides a program and receives information from this application[4]. Driving additional suggests that a larger likelihood that an accident may happen which may lead to costlier insurance premium. Hurst implied that companies like car care sell diagnosable mileage knowledge to insurance corporations. It is vital to notice that once it involves mileage verification, it works each ways; that means updated mileage from a client may result in classifications moving from short to long, or long to short annual mileage notified by Sarkissian [5]. It's a simple matter of probability. The chances of a customer making a claim increases as the car's usage increases. Therefore, premium costs higher if your annual mileage is higher. It's significant to be as specific as possible about the number of miles you drive so that your insurance provider

can more accurately price up your premium. Statistics from the Department of Transport show the average driver of a privately owned car in the UK racks up 7,900 miles annually. Insurance is about risk and to calculate the accurate premium, your insurance provider needs to know as much as there is to know about you and your driving habits. If you mislead your insurance prover to get a cheaper car insurace, your poilcy would be invalidated [6]. Nakamoto et al. studied the use of blockchain in cryptocurrency. The network uses technologies of timestamping with hashing to make it a more efficient system. It also employs blockchain's proof-of-work technique to make it a system with as much accurate ledger as it can. It uses public key cryptography to ensure right payments with other people and to ensure that you've authorized the payment, you sign it with your private key. All computers within the network have a replica of the blockchain which they keep updated by passing along new blocks to each other. In bitcoin, SHA-256 is used as the cryptographic hash function [9]. Haber et al. drafted that all data- text, audio, video being digital in the new age raises the issue of document's original modification date. This requires the data to be time-stamped instead of the medium. A simple time stamping algorithm is by transmitting the document to the Time Stamp Server (TSS). However, there are huge problems such as Privacy, Bandwidth and Storage, Incompetence (file not transmitted fully, etc.), and Trust. They resolved the first two problems using hash values of the file instead of the file. The third problem was solved using digital signature where you send the hash value signed and it responds with date and time appended to it with its signature attached to it. The problem of trustworthiness of TSS is resolved by processes of linking information of previously generated timestamp to every timestamp and also sending a uniqueID of the next timestamp generated so that a user can challenge at any point of time, the validity of the timestamp generated by TSS after its own. The next important step to make TSS more trustworthy is by making it distributive rather than a collective server to make sure no merchant can collude with the TSS to generate fake timestamps [10]. Miller et al. observed that the corporations in industrial sector will adopt to iOT platforms if sensors and actuators become cheaper. Blockchain can modify the sharing of key relevant knowledge captured from the IoT employing a distributed, decentralized and shared ledger that's out there to participants within the business network. How would consumers benefit? Manufacturers, regulators, and suppliers can have correct exposure to component failures on the blockchain and will proactively respond to failure trends more quickly to make sure client safety and satisfaction. The vehicle can firmly obtain supply or repairs mechanically without direct human intervention. The whole record containing information about supply, repairs and payments will be maintained on a blockchain and shared by participants, vehicle owners, makers and finance corporations. Key threshold data encapsulated on the blockchain from the sensors would be used to observe trends for these failures and facilitate proactive maintenance and repairs before the failure happens. The application of analytics and cognitive data produced from the instrumentation on the industrial plant floor can alter reliableness, maintenance, and operations personnel to realize additional careful and correct insight into asset performance.[11]. Kshetri et al. argued that blockchain has a much higher value proposition for the developing world than for the developed world. This is because blockchain has the potential to make up for lack of effective formal institutions—rules, laws, regulations, and their enforcement. In 2017, India's Telangana and Andhra Pradesh states announced plans to use blockchain for a land registry. A land registry pilot project was first started in Hyderabad. It was reported in September 2017 that a complete rollout of the program in Hyderabad and nearby areas would take place within a year. On 14 In October 2017, the Andhra Pradesh government collaborated with a Swedish start-up, ChromaWay, to create a blockchain-based land registry system for the planned city of Amaravati. Blockchain will positively affect developing countries: it can help reduce fraud and corruption and increase legal property titles, which provides entrepreneurial initiatives to the world's poorest [12].Alvarez et al. presented that modern motor vehicle systems are becoming increasingly computerized and vehicle electronics are controlled partially or entirely by microprocessors (computers) networked both from inside and outside. A computing device could generate and transmit telematics data and also receive and process request for telematics data [13]. Singh et al. published that blockchain is making IOT systems more secure but the problem is that IoT devices have low computation power for blockchain. Internet of things is definitely going to be benefited from the functionalities introduced by the blockchain technology through the APIs offered by the nodes of the network or by any specialized intermediaries [15]. Özyılmaz et al. worked on the proof-of-concept implementation for an LPWAN-based IoT deployment to blockchain infrastructure. IoT gateway will push transmitted data to blockchain infrastructure or use BCCAP. They used an intermediary service like a smart

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 11, November 2018

contract that is trusted, which takes the input from the sensor and puts it on blockchain [16].

III. COMPARISON OF HASHING ALGORITHMS

Hashing mechanism provides aspects of information security like confidentiality, authentication, and integrity. Hashing is used to prevent personal data and passwords from being stolen. To be a tool of useful cryptographic value , the hash function must have the following properties:

Pre-Image Resistance- This property prevents from reversing the hash function and revealing its input message.

Second Pre-Image Resistance - It means that for a given intake value and its hash value, there should be no same hash value with the different input.

Collision Resistance - This property indicates that it would require efforts to figure out two different inputs that have the same hash values. There are various algorithms used for hashing. Here we will focus on MD5, SHA1, SHA2, and SHA3.

MD5 produces a 128-bit hash value and is very collision resistant. It takes 60 rounds. It provides fast computation and provides a one-way hash. However, some security vulnerabilities and flaws of MD5 are known and it is also less secure than SHA1.

SHA or the Secure Hash Algorithm is another cryptographic hash algorithm which produces a message digest of 160 bits. It takes 80 rounds.

SHA1 is popularly used algorithm for integrity. It is mainly popular for its time efficiency and robustness. It is a collision resistant and one-way hash algorithm. The size of the output is 160 bits, It takes 80 rounds. SHA2 has two hash functions - SHA-256 and SHA-512. SHA-256 uses 32 bit while SHA-512 uses 64-bit words. SHA-256 produces a 256-bit output and takes 60 rounds whereas SHA-512 produces a 512-bit output and takes 80 rounds. These algorithms are not executed within a same time frame as SHA-1 and are not preferred for integrity. The only drawback of SHA-2 is that it is not time efficient. SHA-3 is different in internal structure and also works with the same hash lengths as SHA-2. It takes 24 rounds. It is not vulnerable to length extension attacks which affect MD5, SHA-1, and SHA-2. SHA-3 can produce an output of 256 or 512 bits and takes 24 rounds. The MD5 algorithm is faster than SHA but is less secure. No complete attacks have been found on SHA so far. SHA algorithms' performance rate is comparatively much better than other cryptographic hash algorithm functions.

IV. DATA COLLECTION

The first challenge towards appending a node onto a structure of blockchain is the content. The data for our model needs to be the Primary Keys, Chassis ID and Odometer reading with the Time stamp. The first problem we encounter is the retrieval of the Distance driven. There are broadly two systems for two different car system, first, an OBD enabled automobile and secondly a modern smart car system. For a not smart car, the kms driven by the car are calculated with an OBD. The sales of the automobiles, since 1996 in the US were made mandatory to have OBD specifications[17]. For our purpose, cars today have the capability of logging in real time through various ports[18]. The entirety of the kms traversed by the subject in consideration can be ascertain with various formulas. For our purpose slight errors are allowed, we chose a simplistic approach. Distance = Engine RPM * Circumference of Tyre per unit time.The frequency can be as per required accuracy. For the tire, the portion of the tyre, that rotates the with the road is variable. The Engine RPM can be queried through the OBD for the specific OBD-PID. The Odometer reading hence is incremented with the Distance value. The smart cars support API. The API can be called to query the distance parameter. Smart car API[19] call to query odometer reading of the target car is - curl https://api.smartcar.com/v1.0/vehicles/{id}/odometer \ -H "Authorization: Bearer {token}" \ -X "GET"The data hence obtained with the use of Wireless Enabled device connected to the OBD or by a call to the API, is stored as a JSON object with the primary key as the Chasis ID. Periodically the data of available objects are uploaded to a node added to the blockchain

V. METHODOLOGY/ PROPOSED SYSTEM

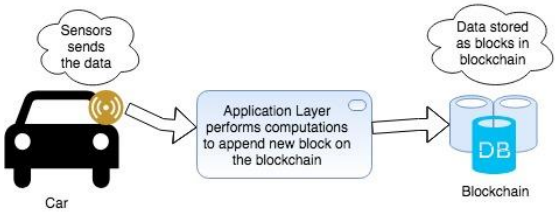

Fig. 1- Three Tier Architecture of Proposed System

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 11, November 2018

The system is consisting of , hardware connected to the wireless device, the distributed blockchain, and an intermediary API layer. The first tier extracts the data and sends it to a server, the API layer does the computation, where the hash is generated and the data block as a node is added to the system i.e. the third layer blockchain. The first tier consists of two separate methods, one for the non-smart automobiles and the second one for the smart vehicles. The odometer reading hence obtained is either the odometer reading or the distance traveled. For the first system, through the previous hash pointing towards the previous node, the cumulative distance traveled can be accessed. For the second system, the odometer reading is considered valid only if the reading is greater than the reading pointed out by the hash value. If the reading doesn't increase for a given time, the distance calculated by the OBD is added to the odometer reading, in case of fraud. This reading obtained for a chassis ID for a particular time

stamp is stored on the server. Periodically a block is generated with the data of all the active automobiles.
Timely updates of the number of kilometers driven are sent to the application interface, after adding the reading values, daily the odometer reading of all the available cars are uploaded as a block and updated to the blockchain with a Nonce value. For every block, a nonce value is generated respectively in the blockchain, wherein it is the primary identification key to that block. Data along with the nonce, a hash is generated. When the block is mined, the hash value according to the settings for the extent of vulnerability set for the encryption algorithm changes. After having been mined, there is a push operation of the block to the chain and a replica of the data structure is sent to each distributed system. In order for a user to modify a previous reading, all the blocks after that block and including that block have to be mined successfully, the algorithm used for consensus working on Stake Proof, hence modifying the chain isn't economically viable. For the contents in a previous block is to be modified, the hash generated for that nonce changes, hence the original block of data is immutable.

This block is updated to the blockchain with a proof to the respective stake validation as it involves low computation power. The block once verified can't be modified. A query can be made by the user for the historical records of the odometer reading of the target vehicle for his perusal.

VI. CONCLUSION

In a marketplace ever booming with second hand used cars, the fundamentals behind trade between the buyer and seller has faded away, leading to losses from both sides our proposed system is a tool to bring back the required trust. With the extensive use of the underlying concept of blockchain, with advanced cryptographic algorithms and a record database built upon majority consensus, our model proposes a record of historical data to be accessed by both the parties for a fair transaction.

VII. FUTURE SCOPE

The applications of decentralized-blockchain technology for the automobile are innumerable. The contents of the blockchain can be utilized by the insurance companies, to analyze the behavior of the driver, hence calculate the premium accordingly. Utilization of IOT and the sensors content leads to further autonomy in the mentioned industry of cars, taking the car for servicing according to the data collected from the sensors, verifying transactions with smart contracts.

REFERENCES

1. The Truth About Blockchain, https://hbr.org/2017/01/the-truth-about-blockchain

2. G. Zyskind, O. Nathan and A. '. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," 2015 IEEE Security and Privacy Workshops, San Jose, CA, 2015, pp. 180-184. doi: 10.1109/SPW.2015.27

3. Dorri, Ali, et al. "Blockchain: A distributed solution to automotive security and privacy." IEEE Communications Magazine 55.12 (2017): 119-125.

4. Chanson, M., Bogner, A., Wortmann, F., & Fleisch, E. (2017, September). Blockchain as a privacy enabler: an odometer fraud prevention system. In Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers (pp. 13-16). ACM.

5. How Car Insurance Companies spy on your mileage,https://splinternews.com/how-car-insurance-companies-spy-on-your-mileage-1793860442

6. How does annual mileage affect the cost of car insurance?, https://www.comparethemarket.com/car-insurance/content/the-effects-of-annual-mileage-on-car-insurance/

7. Supriya T. et al., Blockchain and its applications- A Detailed Survey, International Journal of Computer Applications (0975 – 8887) Volume 180 – No.3, December 2017

8. Eyal, Ittay, Adem Efe Gencer, Emin Gün Sirer, and Robbert Van Renesse. "Bitcoin-NG: A Scalable Blockchain Protocol." In NSDI, pp. 45-59. 2016.

9. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

10. Haber, Stuart, and W. Scott Stornetta. "How to time-stamp a digital document." Conference on the Theory and Application of Cryptography. Springer, Berlin, Heidelberg, 1990.

11. D. Miller, "Blockchain and the Internet of Things in the Industrial Sector," in IT Professional, vol. 20, no. 3, pp. 15-18, May./Jun. 2018.

12. N. Kshetri and J. Voas, "Blockchain in Developing Countries," in IT Professional, vol. 20, no. 2, pp. 11-14, Mar./Apr. 2018.

13. Alvarez, Ignacio, and Mic Bowman. "Trusted vehicle telematics using blockchain data analytics." U.S. Patent Application No. 15/277,066.

14. Crosby, Michael, et al. "Blockchain technology: Beyond bitcoin." Applied Innovation 2 (2016): 6-10.

15. M. Singh, A. Singh and S. Kim, "Blockchain: A game changer for securing IoT data," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 51-55.

16. K. R. Özyılmaz and A. Yurdakul, "Work-in-progress: integrating low-power IoT devices to a blockchain-based infrastructure," 2017 International Conference on Embedded Software (EMSOFT), Seoul, 2017, pp. 1-2.

17. S. Godavarty, S. Broyles, and M. Parten. Interfacing to the on-board diagnostic system. In Vehicular Technology Conference, 2000. IEEE VTSFall VTC 2000. 52nd, volume 4, pages 2000 –2004 vol.4,2000.

18. http://www.scantool.net/.

19. https://smartcar.com/