International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9, Issue-7, May 2020

Blockchain: Security Services Provided for the Accident Detection

Abhilash Kumar, B.Balamurugan

Abstract: ***In the 21st century the traffic congestion is common problem. Due to traffic congestion the accident happened every day. In this paper I proposed to detect the accident on the CCTV camera through video statistics acquisition and image processing and provided the security through the block chain. Now these days it is very important to detect accident video and provided security. Many time people did for own purpose. So always need to provide the security for this kind of CCTV footage in real time. Anyone try and control the video integrity, due to this reason the hash value of the video also change. The hash value is mismatched with the value secure stored inside the blockchain. By using this method, the integrity of video proof cannot be disputable. In this paper, we applied trusted timestamp for verifying the video integrity. Trusted timestamping is an efficient method for verifying unmodified virtual information in a fixed particular point in time. CCTV videos have come to be a valid form of proof in court. Also this method to overcome some of those issues is to get admission to independent facts that such kind of events improves knowledge of what truly occurred in accident. It provides the more and clear information about the accident. After the detecting accident footage decentralized or distributed over the cloud. The security cell gets the data footage or video from cloud. There are the many technique to find detect the accident detection, ex-image processing accident detection, statistics acquisition and image processing ,Adaptive algorithm, Based on the object detection using the machine vision technique.***

Keywords: Blockchain application, trusted timestamp, statistics acquisition and image processing, video integrity, CCTV camera.

I. INTRODUCTION

According the report of World Health Organization approximately 1.2 million people demised each year due to accidents [1]. Extremely good truth is that accident coincidence related deaths is one among the top ten causes of demise internationally, in this list includes tuberculosis, heart sickness and AIDS. And additionally the causalities of accidents provide 1-3% of the world's Gross National Product [2]. In United States, its figure out that vehicle accident approx. 40,000 deaths and causalities price over $164 billion each year. Car crashes accident has majority number of deaths occur [3]. It is predicated that these figure increases 65% over next two decades.

Revised Manuscript Received on May 30, 2020.
***** Correspondence Author
Abhilash Kumar*, Master of Technology, school of Computer science and Engineering, Galgotias University, Gautam Buddh Nagar, Greater Noida, U.P., 201308 India.
Dr. B. Balamurugan, Professor School of Computer Science and Engineering Galgotias University., Gautam Buddh Nagar, Greater Noida, U.P., 201308 India.

The cutting-edge analysis determined that number of hit-run cases increasing each year. According to the NHTSA prediction 737,100 hit and run accident in 2015. [4][5].it predicted that in U.S. hit and run crashes incident happened in every 43 seconds. In 2016 NHTSA recorded the 2,049 casualties from the hit and run crashes. This was best record ever collected by NHTSA [5]. Since 2009, last one decade the causalities have been increasing at a median rate of 7.2%. This is a good method way through which to get admission to independent fact that what really occur during the accident. This record not is keeping as the visitor narrates about the accident. Some people narrate the story yourself to make interesting. But increasing the CCTV camera gets the proper evidence report about the accident, crime and so on many issue. This paper defines clearly to asses that how this kind of source is useful. [6]

Current era tendencies are speeding to embody Distributed Ledger Technology (DLT), in any other case called Blockchain. Blockchain is taking some unique information from a dataset and linked this document immutably. Blockchain is not a new concept; this kind of linking already described in 1991 when a researcher link the file sequentially [7]. Blockchain firstly decided the unique information from the record and linked the information document immutably.

After Santoshi Nakamoto describe the "bitcoin whitepaper" in 2008 [8]. It gives the idea about the "chaining block". This chaining block used to linking the data document. This concept term called blockchain.

Indeed, the particular characteristics of the blockchain, specifically it's allotted and tamperproof developments. Some application of blockchain is for public. In past, blockchain concept secured only the financial record of data. But the recent many applications embody; such like that smart contract which automatically put into effect constant with predefines rules [9]. Many concept define blockchain utility one paper is the "trusted on timestamping of digital data" [10].

In this paper also shows that importance of CCTV camera which accumulated the video and pictures. Increasing the number of the CCTV camera in the urban area mean that increasing information about the accident.

Also avoid the wrong narrated story by the public. The investigators get the video and pictures from thru. And avoid the misleading investigation in the initial stage. The video the content as a separate text file. CCTV cameras have to come to be a valid form of proof in court.

II. BACKGROUND

2.1 Blockchain

The blockchain is a decentralized application.

This application is used for immutable linking of record keeping. Blockchain applied many areas where the integrity of the data is needed. Before that the blockchain is only limited for the cryptocurrency. In 2008 Santoshi Nakamto's define that decentralized and combined maintain ledger important part of the blockchain of bitcoin cryptocurrency [8].

Many researchers define that Blockchain concept is not limited only for the bitcoin cryptocurrency. Blockchain has very huge era when it applied. In 2016, Pilkington paper defines that blockchain with the great potential to "revolutionize the interface among financial dealer" [11].In lastly, they found that Blockchain have "disruptive era". Indeed the blockchain have very unique feature like its tamperproof, it's dispensed, and it's public. It also keeps the nameless data recording. Due to unique feature of blockchain the researcher thinking beyond the financial world. Many researchers have included: one is a smart contract .This application is design with some predefined rules. Blockchain application work put force according to predefined rules and regulation [9]. In 2015, Gipp, Meuschke & Gernandt, build a paper in which the blockchain application depends on the digital timestamping facts [10].Trusted timestamping is a procedure through that defines the unmodified data at a particular point of time. In this paper define how the trusted timestamping used in blockchain [12].

2.2 Key Attributes Of Blockchain Technology

2.2.1. Decentralization

Decentralization is totally different from the centralization. Decentralization provides greater safety and edibility than any centralization application. In the centralization application have done the work on the same place [13] .but in decentralization have done the work on different palace. it has ability to provide the high efficiency output and innovation .here the efficiency tend to save the time and give the higher result. Invitations stand for new idea.

2.2.2. Trust

Trust is an important attribute of blockchain technology. In this application the block carry the information of the previous block. It will work as authentication mechanism path during the transaction. That is why blockchain not need to be third party authentication. Al l the transaction stored in the ledger.

2.2.3Transparent

In blockchain data store transparent. This data cannot be altered in the future. That is reason people have trust on blockchain.

2.3 How Does Blockchain Work?

The blockchain always created a new block through hashing. This new block contents the hash value of the previous block and timestamp of the existing block. So always new block established a connection with the previous block and interlinked with each other. Due to the linking feature, blockchain have no required of third party for the authentication. Each block is interlinked in such way shown in figure 1. Within a blockchain, if any block change the place or order with the other block. It will change the value of hash. It damages the chain of blockchain and created a new shorter chain. This depends on the protocol. The protocol can avoided the shorter blockchain and go through with the longest chain seen in figure 2.

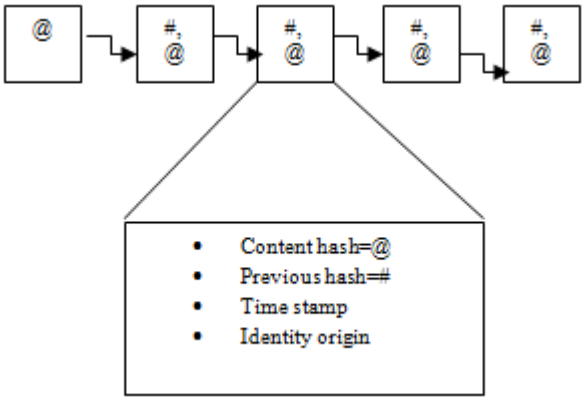

Figure 1. Linking of blockchain

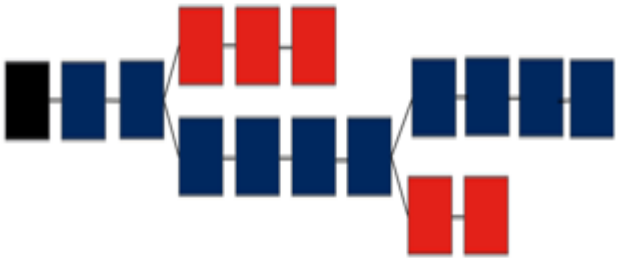

Figure 2. Longest chain of blockchain (blue square box)

The blockchain will keep the blockchain that most people of the customers don't forget to be the ideal one. This may be most of the people of the community if the network is permission less or if the blockchain is permissioned it is going to be most people of depended on nodes. This means that a consensus-based blockchain will maintain the unaltered blockchain. The simplest manner to modify the blockchain is to have the majority of nodes within the machine accept as true with the altered blockchain is the proper one. This would arise if an entity controls greater than half of the computing electricity of the network (in the case of PoW) or if the birthday celebration owns more than 1/2 of the belongings (within the case of PoS). To have one hundred percent control requires one hundred percent of the property of the machine. The fact that each transaction is saved and that nothing is ever deleted or taken out of the blockchain method that the blockchain will continuously grow. Therefore, the blockchain will grow with time and utilization. This consistent increase can create a trouble of scalability for which there is no clean answer. One approach to limit the growth of the blockchain is to usehashes in place of the actual facts. Any quantity of virtual facts can be hashed and the ensuing size of the hash could be no more than 32 bytes (with the use of SHA-256).

III. RELATED WORK

3.1 Timestamping on the mobile recording video

Timestamping concept discuss on this paper "Securing Video Integrity Using Decentralized Trusted Timestamping at the Bitcoin Blockchain" [14].

This paper thesis investigates the applicable scenario for this concept. In this paper, three researchers try to find the use of the bitcoin community to timestamp. The cell phone camera recorded the video which located inside the car. They used the accelerometer of camera to detecting the accident coincidence. If accelerometer value of cell phone exceeds from a threshold value. The app of cell phone initiates to start the recording of video at this particular time. The digital camera of the cell phone processed the output as hashed. This hashed value sent to bitcoin community. The bitcoin community saved the hashed value. Bitcoin community ensured that the no one temper the hashed value. This recorded video use as an authenticate video stored at a particular time of the timestamp.

3.2 Trusted Timestamping

With regards to relied on timestamping reports were identified: "Trusted Timestamping" [15] and Commit coin [16]. Both solutions leverage the time stamp made using the Bitcoin protocol while developing a transaction together with the carbon dating nature of the blockchain (i.e., you'll inform the difficult date of an access via searching at the series of time stamps). These answers are slightly exclusive in phrases of their execution, but the primary theory of using the existing Bitcoin blockchain is the identical. The paper "Trusted time stamping" makes use of a Time Stamping Authority (TSA) [17] on top of the Bitcoin capability. The plain textual content time stamp from the TSA is delivered to the hashed statistics of the transaction and hashed once more earlier than being delivered to the Bitcoin blockchain. Commit coin does no longer use a 3rd celebration to create a time stamp, however alternatively relies totally at the blockchain to do this. Both solutions are based totally upon a block related to the transaction being appended to the blockchain to which subsequent blocks can be appended.

3.3 Forensics Investigations of Multimedia Data

R. Poisel and S. Tjoa paper evaluate state-of-the-art tendencies in forensic investigations of multimedia statistics, like Photographs, motion pictures, and audio files.[18] They defines unique strategies to determine which thing carried out to images and disclose all making information within a images were altered with. To reo determine revealed the construction all the way to determine the images were made for and to temper with the information within a photograph. Being able to tell which element the picture is incompatible with the relaxation of the picture is particular hobby. However, the ability to isolate such disparate factors in an image is scope of this assignment, as we sincerely want to show whether a video collection has been manipulated. However, it is worth noting that using the trendy research done in video forensics would probably be following logical step when investigation of source fabric was also manipulated.

3.4 Digital Watermarking

Digital watermarking is technique through which check the video integrity. I. Echizen defines the work of the digital watermarking on the video files [19].it detect the video file tempering by inserting watermarking in the video. Digital watermarking breaks the video files into different components: video, audio, time code and header. The header and the time code used together with in the digital watermarking. After that the watermarking used on audio and video. After the marking its component are completely mixed and dispatched over the network channel. Because of separating the files, the watermarking can show where the data temper has been done. Video and audio files has been tempered in many ways like deleted, replaced, shifted, header manipulation.

3.5 Industrial Researches

In this paper, three unique industries technology had been discussed as the relevant idea. In this section define only the primary factor of that technology. The blockchain is a new technology securing the data immutably. So many industries work on this technology. Some are discussed below.

3.5.1 Nexan Assureon Archive Storage

"Nexan AssureonTM"Assureon Archive Storage" on which apply an approaches to complete the thesis paper [20]. In that the files record created the fingerprint to show the file integrity inside the archive system. The every unique document is saved on at disks. This document saved at least one disk which keep at different location. This fingerprint of the record used for verify the file integrity. However this is not a longer defines technique to secure the fingerprint.

3.5.2 Enigio - time beat

Enigio product collection "time: beat" consists of: time shot, time stamp, time snatch and time mail from its. This collection of time beat instances share similarities in this thesis. The instance of time beat using an answer of blockchain to archiving time stamped fingerprint of integrity crucial data: email, images, documents and websites [21].

3.5.3 Ascribe

Ascribe used to help those artists, who make the duplicate digital in their painting and timestamp within the bitcoin blockchain. Whenever a document recorded and uploaded. It creates a digital certificate which may be trade, track, or loan through the blockchain. It is an open source protocol which known as "SPOOL" [22].

IV. PROPOSED WORK

4.1 Accident Detection Principle:

Automatically accident detection is itself a challenging method. There are many different technology used for the accident detection. But in this paper accident detect in real time through video statistics acquisition and image processing. It takes the video and picture that specifically define and set in the camera. Camera takes the five pictures per second, and its checks that any change in the picture. When the algorithm analyzer gets the goal information for processing, it generates the coincidence alarm.statistics is transmitting to the inbuilt camera to prepare accident video chunk and calculate the hash value for that video.

4.2 Trusted Timestamping for footage:

In this paper the CCTV utility use of the camera to continuously report video within the historical past whilst the automobile is shifting.

If the smart CCTV camera signs up a sudden collision, only the accident relevant part of video extracted and applied the SHA256 to generate the hash value. The generation of hash value of accident footage to save from future tempering.

CCTV utility right away transmits the hash and video chunk to the VMS. From there VMS transmit the hash to trusted timestamping provider. Origin web Stamp collected the hash value and transfer to bitcoin block. Bitcoin block stored the hash value in tamperproof storage with the minimal cost of bitcoin cope. Hash value tempering almost impossible when it store in the blockchain.

Collision has not to be happen all time. So, some modules of device must be work constantly (see model fig 4). Below define the modules functionality is:

1. Continuously video recording and analyzing.
2. Locate a collision incident the usage of the video statistics acquisition and processing.
3. Create the video files of the relevant "accident detection".
4. Generate the hashed value for that particular accident footage.
5. Video chunk and hash transmit to VMS.
6. VMS transmit the hash for relied on timestamping within the blockchain.

To report the important time of a collision without speedy the use of up tool garage, the software constantly facts sections of video which are quickly stored after which overwritten. If an effect is registered, the utility combines the recording on the time of impact with the temporarily stored older recording, and with the recording from right away after the collision. Since handiest the video photos from around the time of the collision have to be saved, the default video pleasant is ready to maximum.

4.3 Extract the accident video

To prevent the accident video from future tempering. It is needed to extract and secure. By CCTV camera video recording continuous. Below (fig. 3) the diagram this shows how the camera detects the accident detection. If the collision is not detection the video recording continuously .if the collision is detected the video is recorded to generate a chunk file. Once the video documents had been recorded and ordered, a hash is computed of the resulting video document. The variable final Byte includes the records of the ordered video documents in byte shape. The byte shape of the video statistics is hashed the use of SHA-256. This hashing algorithm turned into chosen because it is taken into consideration relaxed in opposition to collision attacks (Gilbert & Handschuh, 2003).

Figure 3.In each second it checking the five

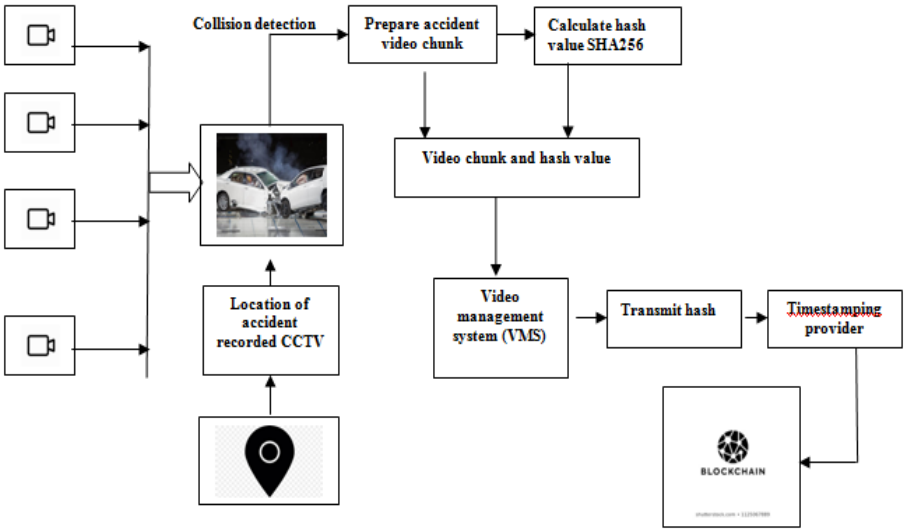

Figure 4. Security provided procedure

Figure 4. Security provided procedure

4.4 CCTV configuration

The results of these tests provide indications of performance and scalability related to the distribution of block arrival sets and records of the system. Managing closed-circuit television (CCTV) evidences at specific coincidences, our check out fence is designed to understand those conditions and focuses on running in a regular networked environment for a range of competence proofs. May be used. IP CCTV based fully transmission; boom mixed with speed will be rapid regulation in the assessment capacity opened huge possibilities for regulation businesses. However, the current nature of CCTV installations has for some time created problems for privacy advocates around the world. This risk has been well tested in both technical and ethical ways.

4.5 Proving video report integrity

To prove the integrity of the accident footage.it hashed must be secured inside the blockchain. The CCTV detects accident and generates the hash value for that particular video chunk. This hashed value must save in the Bitcoin blockchain. If we verifying the chunk integrity. We must check the hashed that is stored in blockchain and hashed calculated of accident footage are same or not. If the hashed value is same, it means that the video file not be altered or tempered. Now there are many inspection tools are available to check the video integrity like: blockexplore.com, blockchain.info.

V. CONCLUSION

To maintain the video integrity of video files are of essential significance, particularly if the video used as evidence.
In this paper proposed the idea how can provided the security in the accident detection video. Paper provided the trusted timestamping for the accident video footage, which sure that the video files was not altered or modify after accident.
Smart CCTV has inbuilt with an application. This application automatically detects the accident incident in real time. The application carried the algorithm of video statistics acquisition and image processing, which detect the accident in real time. After accident detection application make the chunk of particular video files. And calculated the hash value for that particular chunk. The video chunks and hashed value transmitted to video management system (VMS).
VMS sent the hashed value of the chunk to trusted timestamping tamperproof transaction. Transaction ledger which is called blockchain.
Also the courts cannot recognize accident video files as valid evidence. Because the video file may be temper. If the video evidence secured through blockchain, court may be give the permission to use evidence. Because the blockchain provide the immutable security for the evidence. Beyond this hit and run cases accident video also uses as evidence. Increasing the number of the CCTV camera in the urban area mean that increasing information about the accident. Also avoided the wrong narrated story by the public. The investigators get the video and pictures from there. And avoided the misleading investigation in the initial stage. This concept also uses for many purpose. This security also provided in drone, for surveillance and many more.

REFERENCES

1. W. H. Organization, "fact sheet: Top ten causes of death,"factsheetNo.310,2007,www.who.int/mediacentre/factsheets/fs310.pdf
2. Jones, W.D., "keeping cars from crashing," spectrum, IEEE, vol.38, no.9, pp.40-45, Sep 2001.
3. U.D. of Transportation, "Traffic safety facts 2006." *National highways Traffic Safety Administration*, 2006.
4. NHTSA. (2016). National Automotive Sampling System (NASS) General Estimates System (GES): Analytical User's Manual 1988-2015
5. NHTSA. (2017). Fatal Accident Reporting System: Analytical User's Manual 1975-2016.US Department of Transportation.
6. Conche, F. and Tight, M.R. (2006) Use of CCTV to determine road accident factors in urban areas. Accident Analysis and Prevention, 38(6).pp.1197-1207.ISSN 0001-4575.
7. S. Haber and W.S. Stornetta, "How to time-stamp a digital document," *Journal of cryptology*, vol. 3
8. S.Nakamoto, "Bitcoin: A Peer-to- Peer Electronic Cash System," 2008
9. Kosba, A.E, Miller,A. ,Shi,E.,Wen,Z., et al.(2015). "HAWK: The blockchain Model of Cryptography and Privacy- Preserving Smart Contract." *IACR Cryptography ePrint Archive.*
10. Gipp, B., Meuschke,N. and Gernandt,A.(2015). "Decentralized Trusted Timestamping using the Cryptocurrency Bitcoin." In: Proceeding of the conference 2015.March 2015, Newport California.
11. Pilkington, M.(2016). "Blockchain Technology: Principles and Applications." Research handbook on Digital transformation, edited by F. Xavier Ollers and Majlinda Zhegu. Edward Elgar. Swan, M. (2015).
12. Harber, S. & Stronetta, W.S.(1990). "How to Time-Stamp a Digital Document." In: advances Cryptology- Crypto '90 proceeding. Springer Berlin Heidelberg.pp.437-445.
13. (Luon-chang lin1 ,2 and TZU-chun Liao 2) A survey of blockchain security issue and challenges. Jan 2017.
14. B.Gipp, J.Kosti, and C.Breitinger,"Securing video integrityusing decentralized trusted timestamping on the bitcoin blockchain,"MCIS 2016 Proceedings.
15. B.Gipp,N Meuschke, and A. Gernandt,"Decentralized trusted timestamping using the crypto currencybitcoin,"Available:http://arxiv.org/abs/1502.04015
16. J.Clark and A. Essex,CommitCoin:Carbon DatingCommitments with Bitcoin.Berlin,Heidelberg: Springer Berlin Heidelberg. 2012, pp.390-398.ISBN 978-3-642-32946-3.
17. C.Adams, P.Cain,D.Pinkas, and R.Zuccherato, "Intemet X.509 Public Key Infrastructure Time-Stamp Protocol(TSP)," Internet Request for Comments, Vol.RFC 3161(Proposed Standard),Aug.2001.Available:https://rfc-editor.org/rfc/rfc/rfc3161.txt
18. R.Poisel and S.Tjoa,"forensics investigations of multimidea data:A review of the state-of—the-art," in 2011 Sixth International Confarance of IT Security Incident Management and IT Forensics,May 2011.pp.48-61
19. I.Echizen, S.singh, T.Yamada,K. Tanimoto,S.Tezuka, and B.Huet, "Integrity Verification system for the video content by using digital watermarking," in 2016 International Conference on Service System Management, Vol.2, Oct 2016. pp. 1619-1624.
20. "Assureon archive storage data sheet," Available:https://www.nexsan.com/wpcontent/uploads/datasheets/Assureon-ds-v2.pdf,Nexsan,900 E.hamilton Ave.Suite 230,Campbell CA 95008.
21. G oran Almgren, Mats Stengard and "Enigio AB,". Available https://enigio.com
22. Dimitri de Jonghe and Trent McConaghy, "SPOOL," .Available: https;//github.com/ascribe/spool.

AUTHORS PROFILE

Abhilash Kumar, is currently pursuing Master of technology from school of Computer science and Engineering, Galgotias University, Gautam Buddh Nagar, Greater Noida, U.P., 201308 India. He has received B.Tech Computer Science and Engineering from AKU University, Patna Bihar

Dr. B. Balamurugan, is currently working as Professor School of Computer Science and Engineering Galgotias University., Gautam Buddh Nagar, Greater Noida, U.P., 201308 India. He has received Ph.D. degree in (Computer Science and Engineering)-VIT University. He has 13years 3 month experienced in research area and more than 18 years professional experience.