2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE) 978-1-7281-4142-8/20/$31.00 ©2020 IEEE 10.1109/ic-ETITE47903.2020.332

Intrusion Detection in Intelligent Transportation System and its Applications using Blockchain Technology

A.Mohan Krishna
Research Scholar,
Department of Computer Science and Engineering,
Lingaya's Vidyapeeth, Faridabad, Haryana, India.
amkrishna@hotmail.com

Amit Kumar Tyagi
School of Computing Science and Engineering,
Vellore Institute of Technology, Chennai Campus
Chennai, Tamilnadu, India.
amitkrtyagi025@gmail.com

Abstract— **Privacy and Trust are critical issues in automation systems/ transportation systems. Today's Vehicle is need of everyone for moving one place to another. Together this, data security plays an important role in automation systems as critical user's (vehicle's user) data is moved to another user though internet with the help of wireless devices and routes which includes optical fiber, radio channels, etc. In fact, each and every device is connected to the internet and is linked to each other, thus forming the Internet of Things (IoT). As the network is moving towards wireless applications, many threats to vehicles (autonomous vehicles) are becoming a critical problem for vehicles users and service providers. A majority of these attacks can be spotted and detected with the hep of a number of intrusion detection techniques which were elucidated in the earlier decade. These techniques are highly efficient in the identification of any form of individual breaches into the system by catching hold of invalid data access. A few of the systems which need safety are an integral part of Wireless Networks which consist of WLANs (Wireless Local Area Networks), WPANs (Wireless Personal Area Networks), etc. WPAN family further constitutes of three networks which are WSNs (Wireless Sensor Networks), mobile phones and RFID (Radio Frequency Identification like On Board Units (OBUs)). Since digitization is taking place in each and every sector, i.e., defence, healthcare, education, automation industries etc., and so the threat to data also exist. In this article, we protect IoT based environment based smart/ Intelligent Transportation Systems (ITS) using a novel concept "Blockchain Technology". With proposing novel solution called ''PChain using Blockchain Technology (BT), we received many benefit in ITS's applications. We discuss several open issues and challenges for the respective technology in near future (or next decade).**

Keywords— Wireless Sensor Networks, Intrusion Detection System, Internet of Things (IoT), Privacy in Intelligent Transportation Systems, Blockchain Technology.

I. INTRODUCTION

Internet of Things (IoT) which is very often referred to as Internet Connected Things (ICT) has turned to be one of the greatest enhancements in this enormous field of computation. However, the fact that we are trying to grant access to a large-number devices which are clearly heterogeneous makes it hard for holistically handling all these devices and details. Moreover, in order to safeguard the networks, all illicit intruders are to be identified within a specific ground of the network. Intrusion detection, is indeed, one of the topics for extensive research in order to permit access to data and other information to only those who are authorised [1]. When compared to prevention, co-reactance and acceptance of intrusions, intrusion detection is the only one method capable of truly defying plausible cyber-attacks.

A. Intrusion Detection System (IDS)

A method which helps notify the concerned person about the invasion of an intruder, breaching his/her privacy due to which the attacker is blocked, is called Intrusion Detection. At present, Intrusion Detection Systems are categorised as follows:

- Network Intrusion Detection System (NIDS): It mainly brings together all the gadgets which come within the same network and are used for supervising the traffic flowing in from all devices registered under a network.
- Host Intrusion Detection System (HIDS): This involves the supervision of only one particular host device (computers, pc's, etc.) and implements this by monitoring the inflow of data packets and sending alert signals if any malicious activities have been processed.

Methods used for analysis are compared briefly:

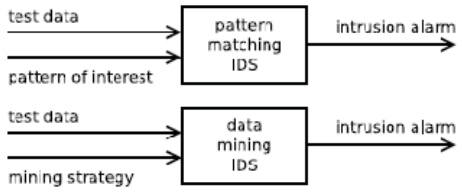

Figure 1: Comparison on the basis of Analysis Techniques

Figure 1 shows that if any intruder is breaching in an environment, that this infrastructure starts alarming.

978-1-7281-4142-8/$31.00 ©2020 IEEE

B. Blockchain Technology

Blockchain is an incorruptible digital ledger of transaction data. Blockchain acts as a distributed database that stores identical blocks of information across its network (means the system has no single point of failure and, because it's distributed, it cannot be controlled by any single node/ user/ entity). Also, a Blockchain network is based on consensus, i.e., it automatically verifies (checks) in with itself at regular intervals/ to verify every transaction that took place during that time frame. These groups of transactions are referred to as 'blocks', hence the name 'Blockchain'. For example, Modex is the first application store for using Blockchain technology [19]. Also, Bitcoin was the first cryptocurrency to use Blockchain in it [3, 6 and 18]. The various benefits of Blockchain within its architecture are listed below:

- It follows decentralised ledger of transaction, in which either no controlling entity is present or a single failure point of the network,
- Since there is no central authority, Every participants have equal rights,
- Since all participants maintain same copies of the ledger, no chance of foul play,
- Fraud and counterfeit can be avoided with the help of high level security and high trust of block chain system,

Note that apart from financial field, Blockchain Technology has great future in other sectors like fraud detection, intrusion detection (cyber security), automation, voting, e-healthcare, etc.

C. Internet Connected Things or Internet Enabled Things

A massive interrelation of objects and devices, machines, instances, etc. capable of data transmission without human intervention forms Internet of Things (IoT devices) [15, 16]. In the same way, taking intelligent transportation or smart vehicles into context, vehicle's internet of things/ internet of vehicles is a group of devices linked to the internet to carry out certain processes supporting the transport sector. Today's s IoT devices in automation/ transport sector have emerged so rapidly and in near future most of vehicle will be integrated to connected through internet (or IoT's devices). Such services will make user's life better and easy to live for a longer duration. Note that small wearable gadgets or implantable sensors in vehicles also a future in automated vehicles. Hence, in [15], author has discussed/ showed integration of IoT devices in many other applications, and have shown a smarter environment for future.

D. Autonomous Vehicles on Demand

There is so much has been written/ discussed (by several authors) about the self-driving in near future (like in 2025/ 2030). In many scenarios, self-driving cars will roam the streets picking up passengers on demand. Note that people can use such service as ridesharing/ carpooling. However, there are many important challenges that must be overcome, i.e., need to be solved with efficient solutions before this become possible, including: secure identity, secure authentication, protection from vehicle hacking, true autonomous vehicles (level 5), and large bias-free datasets, maintaining privacy of passengers/ users all the time. As a reliable solution, these challenges can be overcome by combining Blockchain Technology (immutability, ultra-security, decentralization, and smart contracts), self-sovereign identity, unbiased Big Data, and Artificial Intelligence (AI) and Machine Learning (ML). The next decade belongs to Artificial Intelligence, Cyber Security and Blockchain Technology to solve real world's/ complex problems.

Incorporating Blockchain Technology can ensure that cars are not hijacked remotely, the correct passengers are picked up and charged for rides, identities are not stolen, human preferences are prioritized, and networks become more efficient over time. Each vehicle/ car and each person will likely have a bot assistant which will interact for scheduling, payment, routing, and car preferences. These systems will interact via smart contracts and learn from each other to better customize future rides based on system feedback (i.e., efficiency, cost/time, vehicle usage) and human feedback (i.e., likes, dislikes, preferences). Biometrics (facial recognition, fingerprints) in combination with decentralized car and human identity (private key encryption) will minimize the success of hacking by removing single points of failure. Shared, unbiased big data sets will be required for obstacle categorization and avoidance plus culturally and gender-appropriate human interaction.

E. Smart Vehicular Networks (SVN)

For the autonomous detection of pedestrians and vehicles using sensors, smart traffic lights are implied in the form of smart gateways and is useful for alerting the proceeding vehicles. To multitask, these sensors interact with the adjacent smart traffic lights and manage all the data efficiently. For example, if the sensors spot an upcoming ambulance, they manage the traffic lights in such a manner that they allow the ambulance to pass immediately while putting the other vehicles on a hold. The information acquired from the different traffic lights are further processed locally to provide the necessary traffic management. Furthermore, details from a number of traffic lights (or gateways) are collectively joined and forwarded to the cloud for a global perception on the traffic prevailing in the city. As we know, the costs of our basic needs are gradually increasing day by day and our transport/ transportation system changing very rapidly. Most of people are losing their lives in traffic accidents. Traffic accidents are the result of having maximum vehicles over the road network. Otherwise, a large section of the society/ people are becoming unproductive due to losing their lives. It (maximum accidents) causes a lot to a nation and its economy. The author of [155] has rightly elaborated about the internet of things along with it's compatibility with other forma of applications in the coming years. While the author of [16] have thrown light on the security and safety concerns on this very topic. All such issues may be helpful for further research in the days to come.

Organization of rest of our work is summarized below. All the relevant research work carried out by various researchers was surveyed and summarized in section 2. Factors that motivated us to explore this field are described in Section 3. Our research scope and problem formulation are covered in section 4. Our explored solution is described in section 5. Several concerns and surveys done during the past certain years are dealt in Section 6 .

Finally, this work concluded at section 7 by highlighting the areas for future research.

II. RELATED WORK

The moto of the younger generation today is to fast forward to an era which eases out human tasks more efficiently, one of the best solutions to which is IoT as it's capable of jointly combining internet and other physical instances in an explicit manner [15]. The greater extend to which we are indulged in IoT devices, greater is rise in the problems related to security and privacy. To solve this outbreak, Intrusion Detection Systems, which are safety-security systems applicable on a network layer, were introduced. For the past few years, this has proven to be an essential tool for a global data. As mentioned earlier, Intrusion Detection System is classified as follows:

- Network Intrusion Detection System
- Host Intrusion Detection System

Most of the research works related to intrusion detection systems is explained by Gaudreau and Moorman [4]. Moreover, with reduced price and effectively built computable gadgets, an essence of marketer's module is promoted in the outer regions. The variety of modifications are quite assertive to the IoT generation. With large frameworks beginning from unrecorded ad hoc services to extremely developed standards, IoT seems to be quite skeptical with safety rules and issues. Bissmeyer et al. [20] introduced a signature-based scheme which depends on a plausibility model. Each vehicle is modelled as nested rectangle of different size, and intersecting rectangles that belong to different vehicles represent false position information. Due to inaccuracies of positioning systems such as GPS, the probability of a real intersection is associated with intrusion certainty and trust values by each individual vehicle. Based on number of observed intersections, Intrusion certainty value is calculated. The attack is not identified unless it is above a predetermined threshold. Bouali et al. [21] implemented Intrusion Prevention and Detection System (IPDS), a predictive approach which is capable of identifying multiple misbehaviors before they can occur by predicting vehicles future behaviors. The vehicles are formed into group of one-hop clusters and each cluster has three roles. Firstly, from each cluster the most trustworthy vehicle is elected as CH (Cluster Head). Then each CH divides its range of communication into three equal regions and we select the recommender as the most trusted vehicle closest to each region. The remaining vehicles are monitored by the selected recommenders. The CH permanently monitors the member vehicles and with the help of own observation and information received from recommenders it updates their trust levels. It utilizes Kalman filtering, to detect future attacks. In addition, according to prediction results, the CH classifies the vehicles into white (benign), black (malicious), and gray lists. It is also significant to note that the number of road traffic deaths worldwide was 1.25 million in 2013 [22]. In order to decrease the number of accidents in future different Safety related applications in VANETs such as post-crash notification and road hazard notification are implemented. Zaidi et al. [23], introduced a scheme which depends on statistical techniques to identify multiple misbehaviours. In order to predict and study trends in real traffic flows it uses a model called Greenshield's Model. For each of the messages received, vehicles analyze the mean of the acquired parameters with its own threshold values. If the difference between these seem to be lower than a prescribed value, then the message/data is recognized. Or else, the person who sent the message is closely supervised and the data will be acknowledged only once the collected details are sufficient to carry out a t-test. This test results identify whether the sender is malicious or not. Then, the malicious vehicle will be reported to other vehicles and isolated from the network by rejecting its data. Through his analysis and reports, Robert Mitchell [2], shows that Intrusion Detection is one of the hot topics with a plethora of essential applications. With the complementary support of attack prevention, co-reactance and acceptance, intrusion detection has proven to be one of those ways which has the potential to defy real cyber-attacks which are spoiling important systems. They've acquired the tools and the detection techniques which can be implemented for the same. Furthermore, Mohammed Faisal Elrawy [5] has emphasized on the need for smart surroundings and the driving factor behind their creation which is the spark to ease out human life.

It's to be noted that many attacks which have been spotted in the machines without allowance hovers the privacy of the IoT clients. The safety of such an environment is a matter of concern because of the plethora of attacks and intrusions which have been defined. Works in the near future will focus more on hybrid and mixed nature of IDS for different daises.

IoT, in the current generation has become widespread in a number of fields like medical, urban areas, institutions, etc. This paper has articled the raw truth, that with increased number of connected devices and gadgets to a particular network, the surface has higher chances of brutal intrusions and attacks which are segregated on the basis of the different layers that together form IoT. The security requirements that should be taken into consideration when developing a secure architecture for VANET are authentication, integrity, accountability, non-repudiation, restricted credentials usage, credential revocation, and data consistency. While, the privacy requirements that should be considered when designing a privacy-preserving architecture for VANET are Anonymity, Conditional Privacy, Confidentiality, Unlinkability, Minimum Disclosure, Distributed Resolution, and Perfect Forward Secrecy. Lastly, the system requirements that should be thought of when developing a robust architecture for VANET are Scalability, Storage Requirements, Availability, Real-time Requirements, and Robustness. For Security approaches, two methods are used for providing anonymous services, Group Signature and Pseudonymous Authentication schemes. Both of them address the problem of authentication and privacy. Apart from that, in [13] many requirements for Secure Vehicular Ad Hoc Network have been discussed by Tyagi et al. Also, many attacks/ threats on Internet of Things have been listed out by similar author in [16]. Moreover this, many challenges in Vehicular Ad Hoc Network and its applications like carpooling, toll plaza, parking, navigation services have been listed in [14].

We have also done a detailed survey and analysis on the existing methods of securing IoT and have summed up a few protection methods on the same. Hence, this section basically talked about all the interrelated researches and works done in this arena.

III. MOTIVATION

As per the current situation, almost every industry seems to be shifting towards a system of interconnected things so as to ease their work life and enhance their productivity. However, making use of such devices have raised some stern concerns pertaining to vulnerabilities in software, attacks, etc. To detect these concerns, we need to provide a full detailed record of different intrusions which have taken place. Along with this, we are also required to provide certain information related to IoT linked software and applications like automation during parking of vehicles, etc. [13, 14]. The two types of communication in VANET network are as follows*:* Vehicle to Vehicle (V2V) infrastructure and Vehicle to Infrastructure (V2I). This provides a promising area for the creation of Intelligent Transportation Systems (ITS) which provide assistance and increase safety. Note that smart devices/ IoTs are used in automated vehicles, may cause of leaking privacy of vehicle's user during travelling over the road.
Hence, this section described about the interest towards writing this article and now the next section will describe the open issues and challenges towards intrusion detection system.

IV. PROBLEM DEFINITION

The key issue in Cyber Security [8] is the breaching of data and making use of it in illicit ways. This seems to be an easier and safer method when compared to physically attacking an institute which may result in loss of wealth, time, property, etc. It's of utmost importance to update our systems regularly and secure it especially, if it belongs to any IT sector or medical sector. The reason being, large amounts of medical information are being breached and being sod for lucrative benefits.
The reason behind this much of the medical information is getting stolen and then being sold for money and personal purposes. There are basically two types of attacks:

- Internal Attacks: The internal attack comprises of mainly three kind of problems:
  - Information leakage which is done with the help of an insider.
  - Safety and security of the system and data is a necessity for any establishment.
  - Trust is another crucial factor, especially in the medical field which involves enormous amounts of medical details related to patients and doctors.
- External Attacks: The externals attacks comprises of attacks by ethical hackers, Botnet etc., or by the attack of viruses, Trojan horse etc. These can enter into the system by accessing of any internet site or by attaching any external storage device in the system. Here, attackers are not directly involved with the system. Either they usually track the user's behavior for days or find any vulnerability in the network and then attack whenever they get the appropriate time.

A. Threat Model

In smart parking system, to avail all the services of parking providers, vehicle drivers have to register for that application. Registration driver/ user need to give all his private information to service provider. There is a chance of misusing the driver private information like selling the driver private information to ad agencies. Driver has to give permission to track his vehicle to provide reservations to nearest parking lot. So, there is a possible of jamming attack through road-side units. Using transmitters, the network can jam by attackers which are more powerful then embedded sensors. This attack prevents the Wireless Sensor Network (WSN) gateway's receiving of sensed data, preventing the transmission of information on the status of parking lots to the Road Side Units (RSU). The RSU is therefore not in a position to guide or schedule vehicles in the neighbourhood that are currently requesting parking lots.

B. Internet of Things based Cloud Environment

There are many infrastructures available today like smart infrastructure/ environment using IoT devices, and cyber enabled infrastructure, Blockchain enabled infrastructure, Cloud enabled infrastructure, etc. Few are discussed here as:

a) Cloud based IoT or IoT based Cloud

The vision of IoT can be viewed in ways: Internet centric and thing centric. In internet centric view, services are the key focus. In thing centric architecture object is given the main focus. The main features of this cloud centric frame work are scalability. Different service providers can provision different services like data analysis, data storage, visualization tools etc. The cloud centric IoT framework can offer the services as SaaS, PaaS and IaaS. Here, the cloud computing using Aneka and Microsoft Azure platforms is used to demonstrate how storage, computation and visualization are integrated. Aneka supports Inter-cloud model, so whenever there is a need for additional infrastructure it leases from public cloud. IoT enabled technologies use internet for the communication. IoT cloud is the emerging technology that is being used for many sensor enabled services. This article can be used as a guidance to select a particular cloud platform when developing an IoT enabled service or product. Several articles are found that develop and apply IoT solutions based on the existing clouds that are matter of study in this paper. Strong need for integration of cloud and IoT is mentioned in [16] where an agent-oriented and cloud assisted paradigm is envisaged based on a novel reference architecture. An IoT supported cloud-based smart device is evaluated to perform data monitoring, gathering and processing. Note that IoT based cloud or Cloud based IoT infrastructure have been discussed in [16], in detail.

b) Internet of Vehicles (IoV)

The *Internet of Vehicles* (IoV) is a distributed network which supports the use of data created by connected cars and Vehicular Ad Hoc Networks (VANETs). Basically, *Vehicle to Infrastructure (V2I)* systems supports the wireless exchange of information between a *vehicle* and supporting Roadside Units (RSUs). It is also relate to future vehicular network which includes driving safety, efficiency service, intelligent traffic management, and informative services, etc. In near future, all vehicles will be connected to other smart devices through internet to increase connectivity between users (remote/ non-remote areas). Such communications will produce data in a distributed manner at various servers through suing device to device communication. In near future, all vehicle will be fully autonomous, i.e., vehicles/ cars that are driving themselves.

C. Attacks on Autonomous Vehicles

In [14], several attacks, issues, and challenges have been pointed/ listed out for future research work. Also, similar authors have been tried out to reach with an efficient solution for privacy preserving and building trust, in VANET, by attempting some work which can be accessed at [13, 18, and 24]. Based on the aforementioned security requirements, several attacks should be prevented in the design of security protocols for IoT environment. Some of these attacks include in future vehicles are: Replay attack, Many logged-in users with the same login-id attack, Impersonation attack, Resilience against sensing device capture attack, new comer attack, privileged-insider attack, Denial-of-Service attack, Sybil attacks, MITM (Man in Man Middle) attacks, Password guessing/ change attack, etc. Note that newcomer attack where a node previously identified as malicious can change its IP and enter the network again as a new node. It's to be noticed that the internal and external attacks are harmful to the system in equivalent ways, leading to greater loss of data. At times, there can be chances that the user may not have attacked the system with ultimate intension but may have breached the information accidentally. For example, when a certain employee is replicating data of use and forwarding it to someone and by chance there are possibilities of some other important data being duplicated as well. Hence, this section defines problem in clear manner, including several type of attackers. Now, next section will discuss proposed work (using Blockchain Technology) in detail.

V. PROPOSED SOLUTION

As discussed earlier, it's our duty to safeguard the system from internal and external attacks. Unfortunately, not many of the systems are capable of detecting either internal or external intrusions. In this report, we have put forth an idea which would device a system capable of detecting both type of attacks through this one single device. In most of the systems these days, there's a requirement for password or biometric devices to permit validation and access to important information. Our system consists of two major constituents, RFID (Radio Frequency Identification) and NFC (Near Field Communication). NFC is an activated on-board component which is made use of in vehicles and the corresponding app installed in the smartphone. This app has electronic wallet which is loaded with e-coins. These-coins are generated and stored in encryption mode (using Blockchain), when driver parks his vehicle/ car in a parking lot. The app automatically starts the time period until it exits, accordingly the e-coins are deducted from wallet. This system is more secure for drivers because it doesn't allow to create profiles about driver parking habits and it also against to double spending (a driver can avail more than one parking lot). It reduces payment time. Note that parking lot information is published by publisher (or service provider) and subscriber (customer/ user) is the one who is interested in parking lot information.

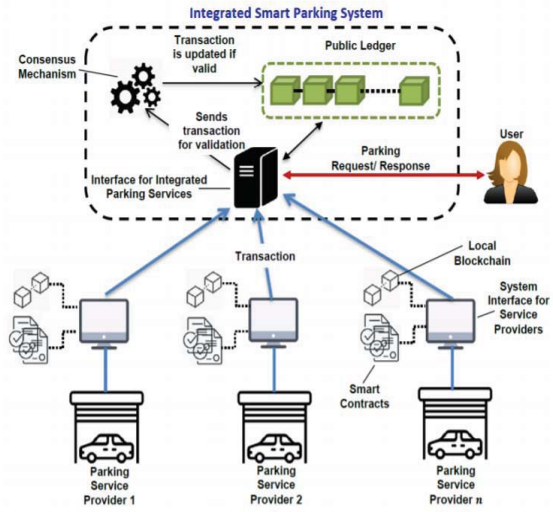

Figure 1: Proposed Model "PChain" for Intrusion Detection in Autonomous Vehicles/ Intelligent Transportation System.

With the help of Transport Layer Security protocol (TLS), these messages are sent between other publisher and subscriber. This model assures confidentiality, authenticity, integrity. In our proposed work, we use decentralized IoT application (i.e., autonomous vehicles which work on wireless sensor network, i.e., on OBU, RSU, etc.) using Blockchain technology. Our proposed model (for parking purpose, in ITS's application) named *'PChain'* operates in a way that no one can delete, hack, revert the time a registered vehicle securely entered a parking area. Blockchain uses cryptography to make secure transactions among various parties without the need of a central authority in Blockchain all the transactions are recorded on a public distributed ledger (public can view all the transactions). Blockchain provides secure broadcasting of encrypted data. This proposed system permits vehicle drivers to securely enter a parking location by taking into advantage Blockchain technology. Here the proposed system deployed and evaluated on the Ethereum Blockchain. In this system, at the entrance and exit of parking location we will install a *Raspberry Pi3* with a camera. Its responsibility is to take photo when vehicle approaches the parking location. Licence plate recognition system uses traditional Image Processing / computer vision approach for licence plate recognition. These number plate in near future can be used to match with authentic data (with government authority) to identify a crime. This approach is classified into two stages.

- Character Localization: It crops the captured image to bottom half because it requires only licence plate number.
- Optical Character Recognition: So as to accomplish low computational cost acknowledgment of License Plate, Morphological Associative Memories (MAMs) which were trained earlier are being used. MAMs without training, it provides character recognition in single pass through a network. Morphological Neural Networks (MNN) represents artificial neural networks whose neurons perform an elementary operation of mathematical morphology, executing smart contract

(checks whether vehicle registered or not), to decide as whether to open the parking barrier or not.

OCR work or number plate recognition process has been discussed by authors in [17]. On the smart contract address, authorized users like admin will be initiating a transaction to register their vehicle to enter into parking location. When a vehicle comes to parking location, camera on the parking barrier captures an image of license plate and with the help of image recognition techniques it will be extracting vehicle registration number (license number). Vehicle registration number is checked in smart contract whether it is registered or not. Barrier will be opened only for the registered vehicles else barrier will not be opened. In summary, this work (proposed algorithm) can be represented in algorithm as:

Step 1: Service provider spread news about free parking slot to public.
Step 2: Customer or user will receive message about free parking slots (region-wise)
Step 3: Customer will select a cluster header (user) in near wise regions
Step 4: Customer will send his/ her information (personal details) to cluster header and will receive a dummy number from cluster header
Step 5: Cluster header will encrypt this information to service provider using asymmetric algorithm 'Digital Signature'
Step 6: Service Provider will use Blockchain Technology to encrypt this encrypted information once again.
Step 7: Once a user occupied a parking place, and leave after a particular time, he/ she will request to cluster header to update the parking status.
Step 8: Cluster header will see status and verify user's identity (after decrypting a block) and complete the payment process.
Step 9: Vehicle user will leave parking place

Note that various benefits are there in our proposed algorithms which are included here as:

a) All transactions recorded after step 6 will be publicly distributed on a network for building trust among vehicular users.
b) Using dummy number, user's anonymity will be maintained, i.e., privacy will be maintained.
c) Encrypting this encrypted information will provide more security and trust among users over a the road network
d) Payment process (at last, at the time of leaving from parking place), will provide satisfaction to user, charge based on used time (about parking place).

Also, some other services will be provided by our proposed systems in Intelligent Transportation Systems' application like

- Real-time parking navigation
- Intelligent antitheft protection (all cars are guarded with RSUs, if any car is moving from parking lot illegally it can be identified by RSUs)
- Friendly parking information distributed to drivers.

Our proposed work/ proposed algorithm can be accessed in pictorial form as figure 2. Hence, through Blockchain technology; we can find internal attackers available in a network. Thus, internal attackers functioning within a network are detected using Blockchain technology. Recognition of internal attack including attackers was a critical matter hitherto but we could resolve this issue easily using Blockchain technology. Coming to the issue of external attack, we will be noticing the intrusion firstly based on the user attempting to login and trying to change the password. On such occasions, our proposed system will be raising an alarm by way of warning to the admn that some intruder is attempting to intrude but when he try to change the password for the second time, the admin will block the user and will keep their information saved. In this section, we have suggested a method for identifying internal attacker and also external attackers in detail. In the next section, we will be elaborating several open issues and challenges in detection intrusion in this smart era or near future.

VI. OPEN ISSUES AND CHALLENGES

Several parameters and mechanisms proposed by Mohammed Amine Ferrage et al [9] for securing IoT deployment are described below: Different mechanisms and parameters must be considered for a secure IoT deployment as described below [9]:

- Confidentiality, Integrity and Privacy of data: Appropriate encoding methods are required for preserving privacy of the IoT information moving over a number of hops in a network. The data preserved on the devices is open to the breach of privacy by the IoT nodes in a network which are prone for compromising due to diversified integration of devices and services in a network. The integrity of the data stored in an attack-prone IoT device is doubtful since the attacker might have changed the stored data for achieving the selfish requirements. For example in case of autonomous vehicle the location data and other passenger/driver data must protect from outsiders to avoid misuse of information.
- Accountability for authorization and authentication: Any network management system(NMS) will have proper accounting procedures for monitoring the resource usage in a network Both authorization and authentication are the biggest challenges in any network on any day including IoT because they are solely responsible for obstructing malicious entry of any type. Authentication of devices in IoT is essential for establishing a communication between two networks and also for securing access to services. The existing IoT authentication process is largely diversified primarily due to non-uniform heterogeneous architecture and environment underneath IoT devices. This is a main hindrance in defining the global standard IoT authentication protocol. The role of authorization is to permit only genuine people to access data and system. Secured communication will be assured if both authorization and authentication mechanisms are properly implemented. In case of autonomous vehicle authentication between vehicle/driver and the passenger is required to avoid unauthorized rides.
- Ensuring services are available: Denial-of-service is one of the most popular method in which all the services are consumed so that required services are not available to the genuine users. To overcome this attack different methods are available like jamming attackers, sink hole

approach. Another cruel approach is to worsen the quality to IoT users.

- SPoF: SPoF refer to the fact that error at any one point bring the whole system completely inoperational. The growing percentage of one-point-failure may cause continuous development of heterogeneous networks for IoT based infrastructure which harm the services ensured by IoT. Possible methods for remedy is to explore different approaches to build fault tolerant network or to build redundant system to take over automatically.

Ahmed Benefa in {10] reported that several benefits are anticipated from Blockchain technology but the below mentioned issues are cause of concern for riping the benefits.

- Difference in storage: Unlike ledger based block chain technology, the requirement of storage in IoT is very less since the information is stored in a single central database. Traditional IoT devices require very little space and therefore central storage is adequate.
- Inadequate facilities: The IoT technology is still nascent and evolving. Multiple issues needs to addressed by appropriate agencies so that IoT could make it presence.
- Human Resource Shortage: Skilled manpower is essential for making any technology acceptable. There is an immediate need to train large number of persons in the area of integrated IoT blockchain concept.
- Government regulations: As on date, there are no laws to regulate this activity. Appropriate agency is required to take up this matter and frame necessary laws on priority basis.
- Request Process time: Available computational facilities may not be uniform and hence the time taken to process each request might vary.
- Expandability: Over a period due to massive usage, the ledger in blockchain might lead to centralization demanding the necessity to maintain different type of records that behave like image to the future blockchain technology.
- Prerequisites:

Also, several challenges (technical and research) towards IoTs based applications have discussed in [7, 16]. Few are listed here as:

- Technical challenges: It is a fact that the IoT technologies and applications are still in their growth face. Many research like, standardization; security and privacy still exist in this area. We must take more efforts in future to overcome these challenges and must explore the features of different industries to make sure that IoT devices fit properly into human centric environments. That is, a keen study about the features and requirement factors like cost, security, privacy, and risk are indeed required before the IoT get accepted and deployed into different domains.
- Research Challenges: Some of the main challenges in Internet of Things are*:*
  - The primary research challenge is to get the correct information at the required level of accuracy.
  - Another problem is requirement of complex tools for Data collection.
  - IoT devices make use of wireless communication they are large introduced at topographically scattered areas. The wireless channels are more prone to distortion and reliability issues. In this situation dependably imparting information without such a large number of retransmissions is a significant issue.

In this subsection we mentioned several future challenges for the implementation of various security protocols in the field of resource constrained IoT environment. Having described various open issues and concerns of current and coming days, it is a time to conclude in the next section about our overall findings with future research directions.

VII. CONCLUSION AND FUTURE ENHANCEMENT

IoT will have a huge potential in diversified disciplines and likely to be adopted by applications of assorted nature. However, IoTs needs to be secured by addressing various types of vulnerabilities that we have listed out in this paper. A ledger based decentralized blockchain concept appears to be an optimal solution for securing data in motion as well as data in rest. In this paper, we have placed our ideas to provide the required security to IoTs based applications/systems and we will be implementing these ideas in real life situations or to the least we will be simulating our thoughts to find the outcome. Further, we have understood the concept of IoV which is a merger of IoT and mobile internet answering the questions pertaining to automobile industry.

Research community is suggested to discover the ways and means to protect IoT and other related security framework like cyber physical solutions with the concept of blockchain. It is ascertained from one of the publication that Microsoft that public blockchain network processing power is prohibilitive to enterprise situations. If that is the case, open source Cocoa Framework proposed in [11] can be explored in detail. However, Blockchain based Platforms to reduce energy consumption while providing more effective and secure services ia need of the hour. Blockchain as a service in an IoT based cloud environments is likely to be accepted by one and all making the decentralized web a reality..

Moreover, Atlam Hany F et al in [12] listed several possible improvements for Internet of Things and also for Blockchain Technology and few important items are (i) The duty of Law enforcing agencies is to find out the culptint and adversaries try their best for escape. The question is how technologies like IoT and anti-forensic exploit adversaries from the security features (ii) how law enforcing agencies and effected persons can gain access to safe, IoT saved communications (iii) If a device is physically controlled and accessible to the public, how the technology ensure security and privacy in IoT device (iv) The dire need of analysis of Bigdata pertaining to automobile industry and use of smart devices.

AUTHOR CONTRIBUTIONS

Both authors A. Mohan Krishna and Dr. Amit Kumar Tyagi conceived this work, with original idea, designed the schemes, and drafted this manuscript.

CONFLICTS OF INTERESTS

The authors declare that there is no conflict of interests regarding the publication of this paper.

REFERENCES

[1] Mishra, A., Nadkarni, K., & Patcha, A, "Intrusion detection in wireless ad hoc networks", IEEE Wireless Communications, 11(1), 48–60. 2004

[2] Robert Mitchell and Ing-Ray Chen, "A Survey Detection in Wireless Network Applications", 2014.

[3] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W., "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies" 2015 IEEE Symposium on Security and Privacy, 11(10): e0163477, 2016.

[4] Audrey A. Gendreau and Michael Moorman, "Survey of Intrusion Detection Systems towards an end to end secure internet of things", IEEE 4thInternational Conference on Future Internet of Things and Cloud, 2016.

[5] Mohammed Faisal Elrawy, Ali Ismail Awad and Hesham F. A. Hamed, "Intrusion Detection Systems for IoT based smart environments: A Survey", Journal of Computing: Advance Systems and Applications, 2018.

[6] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[7] Sathish Alampalayam Kumar and Tyler Vealey, "Security in Internet of Things: Challenges, Solutions and Future Directions", 49th Hawaii International Conference on System Sciences, 2016.

[8] Daryabar, Farid, et al., "A survey about impacts of cloud computing on digital forensics", International Journal of Cyber-Security and Digital Forensics 2.2, 77-94, 2013.

[9] Mohammed Amine Ferrag et al., "Blockchain technologies for the internet of things: Research Issues and Challenges", 2018.

[10] Ahmed Banafa, "IoT and Blockchain Convergence: Benefits and Challenges",2017, https://iot.ieee.org/newsletter/january-2017/iot-andblockchain-convergence-benefits-and-challenges.html

[11] Microsoft 2017,The Coco Framework Technical Overview. https://raw.github usercontent.com Azure/coco.framework/ master/docs/Coco%20Framework%20whitepaper.pdf

[12] Atlam, Hany F., et al., "Blockchain with internet of things: Benefits, challenges, and future directions", International Journal of Intelligent Systems and Applications 10.6, 40-48, 2018.

[13] Tyagi, Amit &Niladhuri, Sreenath. (2017). ISPAS: An Intelligent, Smart Parking Allotment System for Travelling Vehicles in Urban Areas. International Journal of Security and Its Applications. 11. 45-64. 10.14257/ijsia.2017.11.12.05.

[14] A.K. Tyagi and N. Sreenath (2016), "Vehicular Ad Hoc Networks: New Challenges in Carpooling and Parking Services", in proceeding of International Conference on Computational Intelligence and Communication (CIC), Pondicherry, India 2016, vol. 14, (2016).

[15] Tyagi, Amit Kumar, Building a Smart and Sustainable Environment using Internet of Things (February 22, 2019). Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University, Rajasthan, Jaipur - India, February 26-28, 2019. Available at SSRN: https://ssrn.com/abstract=3356500 or http://dx.doi.org/10.2139/ssrn.3356500.

[16] Tyagi A.K., Rekha G., Sreenath N. (2020) Beyond the Hype: Internet of Things Concepts, Security and Privacy Concerns. In: Satapathy S., Raju K., Shyamala K., Krishna D., Favorskaya M. (eds) Advances in Decision Sciences, Image Processing, Security and ComputerVision. ICETE 2019. Learning and Analytics in Intelligent Systems, vol 3. Springer, Cham.

[17] Bansal S., Gupta M., Tyagi A.K. (2020) Building a Character Recognition System for Vehicle Applications. In: Satapathy S., Raju K., Shyamala K., Krishna D., Favorskaya M. (eds) Advances in Decision Sciences, Image Processing, Security and Computer Vision. ICETE 2019. Learning and Analytics in Intelligent Systems, Vol 3. Springer, Cham

[18] Amit Kumar Tyagi, Deepti Goyal "Blockchain Technology - The Necessity of Today's Real – World's Applications for Building Trust", 17-19 July, 2019 in Proceeding of IEEE/ ICCES 2019: 4th International Conference on Communication and Electronics Systems, PPG Group of Institution, Coimbatore, Tamilnadu, India.

[19] Yli-Huumo, J., Ko, D., Choi, S., Park, S., &Smolander, K. Where Is Current Research on Blockchain Technology?—A Systematic Review. PLOS ONE.2016; 11(10): e0163477.

[20] N. Bismeyer, C. Stresing, and K. M. Bayarou, "Intrusion detection in VANETs through verification of vehicle movement data," in Vehicular Networking Conference (VNC), 2010 IEEE, 2010, pp. 166–173.

[21] BT. Bouali, S.-M. Senouci, and H. Sedjelmaci, "A distributed detection and prevention scheme from malicious nodes in vehicular networks," International Journal of Communication Systems, vol. 29, no. 10, pp. 1683–1704, 2016

[22] "WHO | Number of road traffic deaths," WHO. [Online]. Available: http://www.who.int/gho/road_safety/mortality/traffic_deaths_number/en/. [Accessed: 18-Jan-2017].

[23] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection," IEEE Transactions on Vehicular Technology, vol. 65, no. 8, pp. 6703–6714, Aug. 2016.

[24] Tyagi, Amit Kumar and Sreenath Niladhuri. "Providing trust enabled services in vehicular cloud computing." ICIA-16 Proceedings of the International Conference on Informatics and Analytics, Pondicherry, India — August 25 - 26, 2016.

[25] 7907459561