ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

BLOCK CHAIN BASED SECURE DATA SHARING IN VEHICLE SOCIAL NETWORKS

#1**KISHOR KUMAR GAJULA,** *Ph.D Scholar,*
Dept of CSE, Shri JJT University, Rajasthan.

#2**Dr. M.ANJAN KUMAR,** ***Professor,*** **Department of Computer Science & Engineering,**
VIVEKANANDA INSTITUTE OF TECHNOLOGY & SCIENCE, KARIMNAGAR, TS, INDIA.

Abstract: Various services like as traffic management, road safety, and data exchange are made possible through the use of vehicular social networks (VSNs) (videos, audios, roads photos, air quality, and so on). However, because of the broad and complicated network structure, there are new security risks to be concerned about. Data transport is being scrutinised more closely as the use of encrypted transmission continues to grow in popularity. CPABE is the fundamental cypher that is utilised in virtual private networks to facilitate one-to-many data sharing (CP-ABE). Because the access policy is owned and granted by the could, there is a centralising issue about where it is kept and where it is granted. The strategy that we propose has been thoroughly tested and is guaranteed to be effective. User self-certification and cloud non-repudiation are made possible with the usage of blockchain technology. Because we want to be effective, we have developed a certification method that takes into account the capabilities of the vehicle's operator. Although we strongly advise using a security hiding approach owing to the sensitive nature of this information, we strongly advise against doing so. When a car user chooses that they no longer wish to share data, the VSN will remove that data from the system as well. This is the third key advantage of VSNs. After all is said and done, the following conclusion follows logically from the previous sections: Through the use of simulation and analysis, it has been demonstrated that our approach is both secure and efficient.
Index Terms—vehicular social networks, blockchain, CP-ABE, policy hiding, data revocation.

1. INTRODUCTION

The variety of automobiles found in cities, as well as the variety of vehicle limitations, pose a number of obstacles, including traffic congestion, traffic accidents, and other issues. Vehicle-to-vehicle networks (VSNs) have the potential to play a significant role in passenger-focused networks, in which vehicles communicate with one another and with infrastructure in order to improve traffic safety and reduce traffic congestion. Citizens will also be able to access social services through these networks, which will be beneficial to them. Because of the potential benefits of this industry, major information technology companies have already begun investing in its development and testing.

Apple's Carplay vehicle-interface technology, which was announced in March of this year, provides an example. It's also crucial to remember that Google has made significant investments in the development of virtual spectacles, which were first revealed in June 2014 as part of the Android Auto virtual glasses programme. Vehicle sensor systems, which may include sensors for everything from sound detection to acceleration detection, are typically fitted in VSN vehicles. The terms "vehicle-to-vehicle" and "vehicle-to-infrastructure" are used to refer to communications between vehicles and infrastructure, respectively. Vehicle-to-vehicle

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

(V2V) and vehicle-to-infrastructure (V2I) communications are also referred to as "vehicle-to-infrastructure" communications. Vehicle sensor nodes (VSNs) are really car-based computers that collect vehicular sensory data and transfer it to a vehicle cloud server that is located within the vehicle itself. The consideration of delicate sensory data such as traffic data, personal data, and vehicle information necessitates the consideration of issues of security and privacy.

Data privacy and security have long been considered straightforward issues, with the preceding recommendation of encrypting sensitive vehicular sensory data and granting separate access privileges over encrypted data that uses various encryption keys as a means of addressing the issue. There is still no solution to the problem of how to allocate access privileges for numerous encrypted data types that use different encryption keys, which hasn't been resolved yet. For example, providing motorists with traffic-related information is a job that vehicle drivers perform. Traffic information that is tailored to each customer's needs is appropriate for consumers who live in different locations and have a variety of needs for their automobiles. Owners of vehicle data can use the vehicle sensing data, as well as the KAE and KASE primitives, to do selective one-to-many data sharing with other vehicles.

Because automotive data users do not want or require information about all search results, KAE approaches must return the entirety of all matched search results. Unfortunately, this is the only option available. By keeping the secret key up to current and easily accessible to users, vehicle data owners can allow several users to view different encrypted data files at the same time. Users will be able to search for and access encrypted material in this manner while keeping the key secret. In the near future, it is hoped that this issue will be remedied successfully. Plaintexts can be recovered even when the private key is unknown since existing KASE software has keyword privacy leakage, which allows plaintexts to be recovered.

KASE does not now offer a selective and secure data exchange solution, nor does it intend to do so in the future. Because of the instability of the KASE, it has been impossible to build a legitimate VSN situation in the intervening time period.

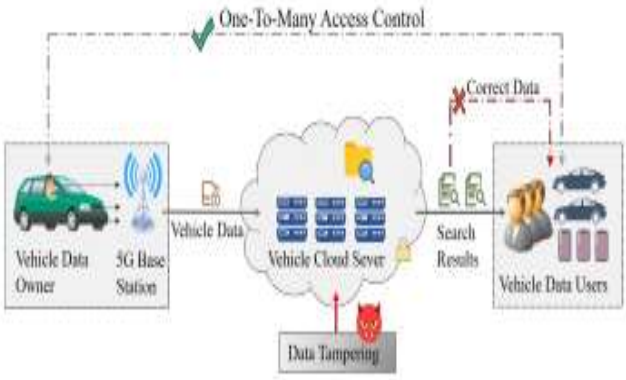


Fig. 1: Security challenges in vehicular social networks

Furthermore, there is currently no certified searchable data sharing solution available for KASE that is capable of integrating blockchain technology effectively. When it comes to VSNs, the number of security issues that they face is staggering. Fig. 1: A diagram of the human body. On-board car cloud servers save information about the vehicle in an encrypted format. When drivers make changes to the data that has been stored, they have the option of uploading a new version. Personal responsibility for fatal accidents and traffic conflicts both urge those who are at fault to alter sensory data in order to avoid criminal prosecution or financial compensation, while also protecting their public image in the process.

It is possible that data stored by an automotive cloud server will be tampered with if the server, for example, is used to assist accident victims in their compensation claims. Because of this, it is essential that the vehicle's stored data is not tampered with in any way. The retrieval of erroneous keyword-based ciphertext has a significant impact on the quality of search results, and it has even been linked to traffic accidents. Make certain that no inaccurate search results are offered in order to aid in the prevention of wrong results being returned. As a result, it is critical to

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

examine the return value of the automotive cloud server for users of automobiles before using it. Despite the fact that some organisations have invested time and resources into developing a plan to deal with data tampering or confirmed recovery, no existing plan is capable of dealing with the wide range of issues. To summarise, the combination of the two objectives of data tamper resistance and query verification raises the total difficulty level of the problem.

2. BACKGROUND

2.1 Internet of Vehicles

ad hoc grouping of automobiles that forms on the fly (VANET). IOVs will enhance the benefits of using VANETs, but new technology will also come into play and assist in overcoming the obstacles that VANETs will encounter in the future. IoVs and VANETs are compared and contrasted from a variety of perspectives, and it is proved that they both have significant advantages when it comes to the design and development of networks. In order to accomplish vehicle-to-vehicle (V2V) communication, roadside sensors (RSUs) must be installed on the roadside. With VANETs, ten distinct traffic safety and efficiency issues can be addressed at a cheaper cost than they would be otherwise. The VANET IoVs develop as a result of the commercialization restrictions placed on VANET technology, such as unstable Internet access and device incompatibility, which are imposed on the technology.

RSSUs are examples of communication devices that are more market-oriented and complicated in the Internet of Things communication architecture. In order to make connections between vehicles, infrastructure, devices, and sensors smarter, the Internet of Vehicles (IoVs) is attempting to make connections between vehicles, devices, and sensors smarter. The transition from the VANET to the IoVs was necessitated by the VANET's inability to handle and analyse the growing amount of data generated in the automotive environment. When compared to the Internet of Vehicles, the VANET can provide services such as vehicle safety and traffic management.

The Internet of Things (IoT) is a larger network than the VANET, and the VANET is a sub-network of the IoT. Network technologies such as SDN, EC, and NFV help to increase performance on the Internet of Things (NFV).

Despite the fact that the IoV significantly exceeds the boundaries of the VANET, entities can nevertheless cause harm to the IoV in a variety of ways. Although some Internet of Things obstacles, such as data authentication security, vehicle privacy, and resource availability, are still significant issues, others, including as interoperability, transport security, and reliability, are not as widespread. When diverse technologies are integrated into the IoV architecture, there are a few problems that must be addressed. In order to encourage automobiles to participate in the process of data sharing and resource scheduling, incentive mechanisms must be included.

2.2 Blockchain

Blockchain technology underpins the Bitcoin blockchain, which served as the catalyst for the revolution. In the blockchain, every bit of information is identical and cannot be changed. A public key that represents a person's identity makes it difficult to determine who that person is. This word refers to the likelihood of this platform resulting in the creation of a decentralised, transparent, irreversible, and secure data storage environment, which is what it implies. For each transaction to be executed on the blockchain, each node generates a block of data and distributes the block to other nodes, where the transaction information is recorded and validated by all participants on the network. Figure 2 depicts a block diagram of the block structure. Blocks can be divided into two types: block headers, which contain metadata and transaction data, and transaction blocks, which contain transaction data. The hash of the block before Te is included in the metadata of the Te block header.

The current time, mining difficulty, and random number creation are all included in this section (Nonce).

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

a cryptography system There is a tree called Merkle Tree.

Several different consensus algorithms have been developed for use in the consensus process, including Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPOS), Practical Byzantine Fault Tolerance (PBFT), Ripple, and Paxos, among others. Table 1 contains some examples of typical consensus application scenarios to serve as illustrations of the numerous common consensus application scenarios. It was originally designed only for the purpose of facilitating the exchange of digital currencies, and it did not feature smart contracts at the time of its creation. Smart contracts are generated using Szabo's trustless digital contract, which is a trustless digital contract with no trust. When it comes to smart contracts, the majority of people are familiar with the fact that they are built on regulations and applied automatically. These more recent systems, like as Bitshares and Stellar, have the ability to handle smart contracts in the same way as Ethereum and Hyperledger do. Individuals can use these platforms to construct a multitude of different services, apps, and contracts once they have been developed. Blockchains can be classified into two types: public and private.

Fig. 2 Data structure of blocks

3. SECURITY ANALYSIS

A. Data Confidentiality

CP-ABE is the system that we utilise because we built it ourselves (which has been demonstrated to work). The DUs (whose origin and function are still a mystery) are barred from entering the country (56). As long as the DUs have the appropriate properties to fulfil the CSP's access control criteria, the CSP deciphers the ciphertext in advance, allowing the CSP to perform a pre-decryption of the ciphertext. It is critical to understand that blockchain data is saved using a hash value, hence it is necessary to understand what that value is. This has resulted in our solution determining that what we claimed was right, and as a result, our approach is able to resolve the issues associated with bogus DUs. To be sure, even though the CSP does not have access to DUs' attributes, DUs in the cloud retain their decryption secret keys for those properties that may be accessed. We put our faith on CAs to keep the decryption keys that DUs are entrusted with a secret from anyone else. The ability of the CSP and CA to work together is hampered as a result of this. This also implies that the CSPs are responsible for adhering to the confidentiality duty.

B. Collusion Attack Resistant

This criminal network is made up of criminals who cooperate to breach encrypted data in order to steal the information contained within it. According to CBM X YZ (), only those who hold the X Y or the X Z have access to the information. An attribute-value pair user is distinct from an attribute-value pair user who possesses both qualities X and Y, as described above. In order to decode the cypher, A and B must work with one another, which they are unable to do as a result of their differences. When attempting to create near-duplication of A, B is the chemical that can be used. It is our sole and exclusive property that each user has a unique ID that is linked to their attributes and decryption keys. The CSP does not

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

pre-decrypt the ciphertext using the CSP attribute secret keys when many users are involved in the encryption process. We've noticed that following this advice can help to reduce the amount of collaboration among the users in the workplace. It's also worth noting that, in a different context, CSP formed a contact with the illegal immigrant population. Users that have access to the encrypted ciphertext are provided with encrypted ciphertext in order to aid them in deciphering the ciphertext they have access to. Their understanding of the crucial key is limited, but they are certain that the information is secure. There is no way to recover any of the data. In order to make it apparent that our technique is secured against the CSP as well as collusion by end users, the previous comment has been modified.

C. CSP Attacks Resistant

CSP gains the credibility of a third party as a result of CP-ABE. It's following our protocol, but it's also interested in the information we're providing. In theory, cloud service providers (CSPs) should not interfere with data integrity or deny access to any particular user. The present CP-ABE methods are not designed to address these difficulties. We use the blockchain to track and maintain the hashes of medical data, such as patient treatments, that are entered into our platform. The user can then proceed to section V.A. to complete the "Verify DU2" command, which is found after the CSP has completed the request. In the event that data tampering occurs, the CSP will provide you an error message. He must take action in order to verify the facts. We are not affected by inaccuracies in data because our technique is protected from them thanks to the CSP. It was built with regulations in mind, in order to protect any sensitive information that might be stored on it. Before proceeding to the next step, the user must first complete the Verify DU1 command in Section V.A. of the manual. The CSP will still return a value that is not a number (NaN). If this occurs, a CSP error report will be generated and provided to the user. It is feasible that the CSP will no longer reject valid user access data as a result of the implementation of this new approach.

4. PERFORMANCE ANALYSIS

Simulating the computational time required for encryption and decryption would be similar to simulating the time required to compute a solution in Chase's system [23] and Fan's method [41]. Systems such as Chase's and other CP-ABE systems are frequently encountered. While the fan technique is effective for both encryption and decryption, it can also be used to aid in the application of rules. Our technique took advantage of the Python programming language, which is a platform designed to allow developers to prototype cryptographic schemes and protocols, and we implemented it using the Charm [57] library of libraries.

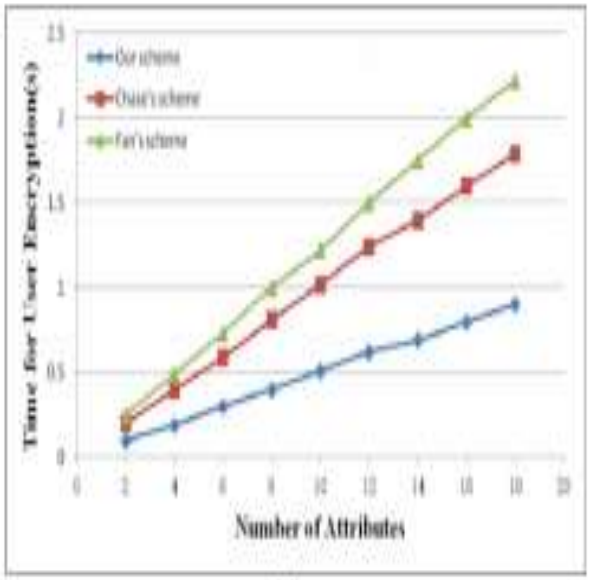
We used an Intel(R) Core(TM) i5 processor with 4GB of RAM running Ubuntu 14.04 64-bit and Python 2.7 to perform the encryption, decryption, and revocation operations. As shown in Fig. 4, each object under the control of an AA management system has ten characteristics and is 1,000 bytes in plaintext. This graphic, for example, indicates that encryption time increases linearly with the number of characteristics and that it typically ranges between 0.1 and 1 second per attribute in most cases.

Because of the usage of outsourced decryption, the decryption time for user accounts remains at approximately 0.2 seconds with this technique. This leads to the obvious conclusion that the amount of time necessary to encrypt using our technology is less than the amount of time required by the other two methods. The usage of our technology will result in less computational power being consumed, which will result in fewer bilinear maps and exponential operations being performed during encryption.

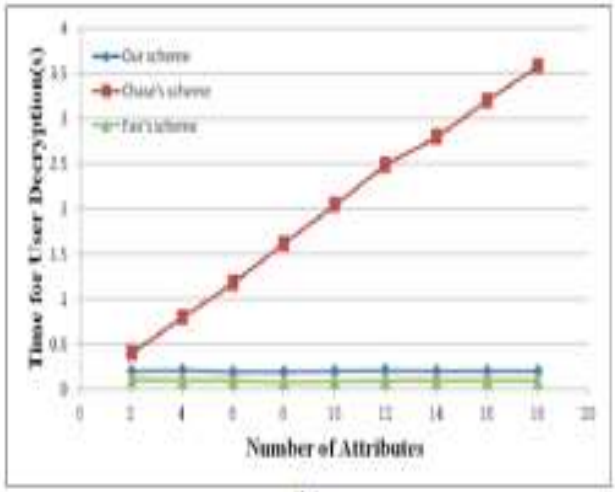
However, the time it takes to decode our technique is substantially less than the time it takes to decrypt Chase's, which is a big advantage. Calculations such as decryption must be

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

conducted during the decryption phase as a result of this limitation on time.



(a)



(b)

Fig. Time cost for user with different number of attributes. (a) Encryption time; (b) Decryption time.

As depicted in Figure 5, the expenses associated with preserving data revocation are clearly visible. With the help of the CBM and CSP, it is possible to compute and confirm a signature in less than 0.3 seconds. The CBM is responsible for developing the final product in order to complete the transaction successfully.

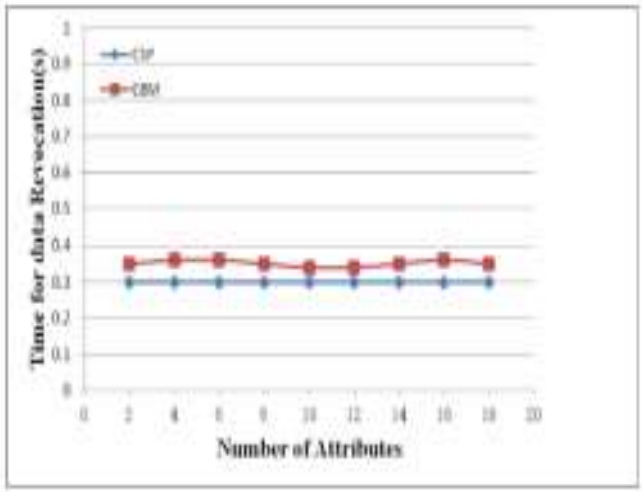


Fig.. Comparison of time cost for CSP and CBM in the data revocation process.

5. CONCLUSIONS

In Virtual Smart Networks, a verifiable and secure data exchange system that integrates both CP-ABE and blockchain has been shown using both technologies (VSNs). In order to facilitate data sharing in a one-to-many format, we developed a system that makes use of the CP-ABE protocol. We have also utilised blockchain as a method for storing permission access data, assuring users self-certify, and providing them with proof of non-reproach in the cloud, all at the same time. We have created an effective validation procedure to ensure that the processing capabilities of the VSNs node is sufficient. The implementation of a technique for concealing sensitive data within the access policy has been completed. Deletion feature is also available, allowing you to remove your content from the internet whenever you choose. Both the simulated trials and the security investigation provided evidence in support of our recommended approach. Using data analysis, we will look into how we may reduce the amount of time it takes to establish an agreement in future.

REFERENCES

❖ L. Fan, and Y. Wang. "Routing in vehicular Ad Hoc networks: A survey." IEEE Vehicular Technology Magazine, vol. 2, no. 2, pp. 12-22, 2007.

ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

❖ J. Wu et al., "FCSS: Fog computing based content-aware filtering for security services in information-centric social network." 1-1, 2017.
❖ K. Zhang, X. Liang, J. Ni, K. Yang, and X. Shen. "Exploiting social network to enhance human-to-human infection analysis without privacy leakage." IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 607-620, 2018.
❖ Qu, F.; Wu, Z.; Wang, F.; Cho, W. A Security and Privacy Review of VANETs. IEEE Trans. Intell. Transp. Syst. 2015, 16, 2985–2996.
❖ Boualouache, A.; Senouci, S.; Moussaoui, S. A Survey on Pseudonym Changing Strategies for Vehicular Ad Hoc Networks. IEEE Commun. Surv. Tutor. 2018, 20, 770–790.
❖ IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture; IEEE Std; IEEE: Piscatawat, NJ, USA, 2019; pp. 1–219.
❖ Intelligent Transport Systems (ITS); Communications Architecture. Available online: https://www.etsi.org/deliver/etsi_EN/302600_302699/302665/01.00.00_20/en_302665v010000c.pdf (accessed on 4 November 2020).
❖ Vegni, A.M.; Loscri, V. A Survey on Vehicular Social Networks. IEEE Commun. Surv. Tutor. 2015, 17, 2397–2419.
❖ Wang, X.; Ning, Z.; Zhou, M.; Hu, X.; Wang, L.; Zhang, Y.; Yu, F.R.; Hu, B. Privacy-Preserving Content Dissemination for Vehicular Social Networks: Challenges and Solutions. IEEE Commun. Surv. Tutor. 2019, 121, 1314–1345.
❖ Y. Kawamoto, N. Kato, et al., “Toward Future Unmanned Aerial Vehicle Networks: Architecture, Resource Allocation and Field Experiments”, IEEE Wireless Communications, vol. 26, no. 1, pp. 94-99, 2018.
❖ D. Chen, N. Zhang, R. Lu, et al., “An LDPC code based physical layer message authentication scheme with prefect security”, IEEE Journal on Selected Areas in Communications, vol. 36, no. 4, pp. 748-761, 2018.
❖ J. Sun, H. Xiong, et al., “Mobile access and flexible search over encrypted cloud data in heterogeneous systems”, Information Sciences, vol. 507, pp. 1-15, 2020.
❖ Rahim, X. Kong, F. Xia, Z. Ning, et al. ,“Vehicular social networks: A survey”, Pervasive and Mobile Computing, vol. 43, pp. 96–113, 2018.
❖ Vegni and V. Loscri, “A survey on vehicular social networks”, IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2397–2419, 2015.
❖ J. Ning, N. Kato, et al., “Attacker Identification and Intrusion Detection for In-vehicle Networks”, IEEE Communications Letters, DOI: 10.1109/LCOMM.2019.2937097, 2019.