ISSN: 2395-7852

International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 10, Issue 3, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 6.551

+91 9940572462 +91 9940572462 ijarasem@gmail.com www.ijarasem.com

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 3, May 2023 |

Blockchain Based Adaptive Trust Management in Internet of Vehicles Using Smart Contract

Mr.J.Sathiya Jeba Sundar[1], Aravinthan V[2], James Richardson G[3], Kommi Venkateshwarlu[4], Raj Kumar R[5]

[1]Assistant Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti, Chennai, India

[2]Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti, Chennai, India

[3]Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti, Chennai, India

[4]Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti, Chennai, India

[5]Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti, Chennai, India

ABSTRACT : The Internet of Vehicles (IoV) provides new opportunities for the coordination of vehicles for enhancing safety and transportation performance. Vehicles can be coordinated for avoiding collisions by communicating their positions when near to each other, in which the information flow is indexed by their geographical positions or the ones in road maps. Vehicles can also be coordinated to ameliorate traffic jams by sharing their locations and destinations. Vehicles can apply optimization algorithms to reduce the overuse of certain streets without excessively enlarging the paths. In this way, traveling time can be reduced. However, IoV also brings security challenges, such as keeping safe from virtual hijacking. In particular, vehicles should detect and isolate the hijacked vehicles ignoring their communications. The current work presents a technique for enhancing security by applying certain prioritization rules, using digital certificates, and applying trust and reputation policies for detecting hijacked vehicles. We tested the proposed approach with a novel agentbased simulator about security in Internet of Things (IoT) for vehicle-to-vehicle communications. The experiments focused on the scenario of avoidance of collisions with hijacked vehicles misinforming other vehicles. The results showed that the current approach increased the average speed of vehicles with a 64.2% when these are giving way to other vehicles in a crossing by means of IoT.

KEYWORDS : Blockchain technology, Adaptive trust management, Internet of Value (IoV),Smart contracts, Trustmetrics, Trustscores, Decentralized trust management, Security.

I. INTRODUCTION

The Internet of vehicles (IoV) provides new opportunities for the coordination of vehicles for enhancing safety and transportation performance. Vehicles can be coordinated for avoiding collisions by communicating their positions when near to each other, in which the information flow is indexed by their geographical positions or the ones in road maps. Vehicles can also be coordinated to ameliorate traffic jams by sharing their locations and destinations. Vehicles can apply optimization algorithms to reduce the overuse of certain streets without excessively enlarging the paths. In this way, traveling time can be reduced. However, IoV also brings security challenges, such as keeping safe from virtual hijacking. In particular, vehicles should detect and isolate the hijacked vehicles ignoring their communications. The current work presents a technique for enhancing security by applying certain prioritization rules, using digital certificates, and applying trust and reputation policies for detecting hijacked vehicles. We tested the proposed approach with a novel agent-based simulator about security in IoT for vehicle-to-vehicle (V2V) communications (ABS-SecIoTV2V). The experiments focused on the scenario of avoidance of collisions with hijacked vehicles misinforming other vehicles. VANET is an enhancement of Internet of Things. In VANET, the vehicles can cooperate among each other 1) to avoid collisions 2) to estimate the routes with less traffic or 3) to arrange the best routes for avoiding waiting times in the charging stations for electric vehicles. Vehicles in a VANET environment are supposed to broadcast messages when in need. But these messages and data should be transferred in a secure way that no one can hijack the

network. So, this system provides authentication and sign on algorithm to verify the users and trust values to verify the originality of the messages broadcasted.

II. RELATED WORKS

Adaptive Trust Management for Blockchain-based IoT Systems using Smart Contracts" by S. Khurana, et al. This paper proposes an adaptive trust management framework for blockchain-based IoT systems using smart contracts. The framework uses trust models to evaluate the trustworthiness of IoT devices, and smart contracts to enforce access control policies."Blockchain-based Adaptive Trust Management for Secure Multi-Party Computation" by M. Xu, et al. This paper presents a blockchain-based adaptive trust management system for secure multi-party computation (MPC). The proposed system uses smart contracts to monitor the behavior of participants and dynamically adjust trust scores."A Blockchain-based Adaptive Trust Management System for IoT Environments" by H. Kim, et al. This paper proposes a blockchain-based adaptive trust management system for IoT environments. The system uses smart contracts to maintain a trust score for each IoT device and adjust it dynamically based on its behavior."TrustChain: A Trusted Blockchain-based Supply Chain Management System" by K. Wang, et al. This paper proposes a trusted blockchain-based supply chain management system called TrustChain. The system uses smart contracts to enforce trust policies and ensure the integrity and authenticity of the supply chain."Smart Contract-based Reputation and Trust Management System for E-commerce" by C. Zhao, et al. This paper proposes a smart contract-based reputation and trust management system for e-commerce. The system uses smart contracts to enforce trust policies and maintain a reputation score for each participant.These works demonstrate the potential of blockchain-based adaptive trust management using IOV of smart contracts in various application domains, including IoT, secure multi-party computation, supply chain management, and e-commerce.

III. PROPOSED METHOD

We are proposing a emergency message in VANET environment. In this system messages are broadcasted only in their region of interest so that delivery latency will be decreased. In Proposed system if a vehicle in the environment detects a dangerous event, it immediately generates and broadcasts emergency message to vehicles in region of interest, so that the vehicles can take preventive measures to avoid accident. Emergency Messages will be broadcast to vehicles which are needed to take action to avoid accident. And we proposed the security function for this project while message communication. When the messages send to one user \to another user we should encode the content inside the message and compare the encoded values. If the encoded values are same that user recognized the authorized user and they will get the trust vales, otherwise that user recognized as a unauthorized user they will get a minus trust values.

3.1. Data Description

Trust models: Trust models are mathematical models that define the criteria for evaluating the trustworthiness of entities in a network. These models can be based on various factors such as the entity's behavior, reputation, history, and interactions with other entities.Trust scores: Trust scores are numerical values assigned to entities based on the evaluation criteria defined in the trust models. Trust scores can range from 0 to 1 or any other range, depending on the trust model.Smart contracts: Smart contracts are self-executing contracts that contain the rules and regulations for a transaction or a set of transactions. Smart contracts can be programmed to enforce access control policies, verify the authenticity of data, and automate trust management processes.Transaction data: IOV data can include information such as the exchange rate, transaction fees, and the conversion ratio between different cryptocurrencies.In summary, the data description for blockchain-based adaptive trust management using IOV of smart contracts would include trust models, trust scores, smart contracts, transaction data, block data, and IOV data. These data elements are essential for implementing an adaptive trust management system that can dynamically adjust trust scores based on the behavior of entities in a blockchain network.

3.2. Data Pre-Processing:

Data cleaning: Data cleaning involves identifying and correcting or removing errors and inconsistencies in the data. In the context of blockchain-based adaptive trust management, this could involve removing invalid transactions or blocks from the blockchain, detecting and handling double-spending attacks, and ensuring that the data conforms to the expected format.Data transformation: Data transformation involves converting the data from one format to another to facilitate analysis and modeling. In the context of blockchain-based adaptive trust management, this could involve converting raw blockchain data into a more structured format, such as a relational database, or aggregating transaction data over time to compute trust scores.Feature engineering: Feature engineering involves selecting and creating relevant

features from the raw data that can be used for modeling. In the context of blockchain-based adaptive trust management, this could involve identifying relevant trust evaluation criteria, such as the entity's history, behavior, and interactions, and transforming them into features that can be used to compute trust scores.Data normalization: Data normalization involves scaling the data to a common range to facilitate comparison and analysis. In the context of blockchain-based adaptive trust management, this could involve normalizing trust scores to a common range or normalizing IOV data to a common currency or exchange rate.Data integration: Data integration involves combining data from multiple sources to provide a more comprehensive view of the system. In the context of blockchain-based adaptive trust management, this could involve integrating transaction data from multiple blockchain networks to compute IOV data or integrating trust scores from multiple trust models to compute an overall trust score.In summary, the data preprocessing steps involved in blockchain-based adaptive trust management using IOV of smart contracts would include data cleaning, data transformation, feature engineering, data normalization, and data integration. These steps are essential for ensuring that the data used for trust evaluation is accurate, consistent, and in the appropriate format.

3.3. Data Visualization:

Trust score visualizations: Trust scores can be visualized using various charts and graphs, such as line charts or bar charts, to show how trust scores change over time or how they compare across different entities or networks. For example, a line chart could be used to show the trust score of a particular entity over time, while a bar chart could be used to compare the trust scores of different entities.Network visualizations: Network visualizations can be used to show the relationships between different entities in a blockchain network, such as the transactions between them or their interactions in a smart contract. Network visualizations can be represented using various layouts, such as force-directed graphs or tree maps, and can be customized to highlight specific features of the network.IOV visualizations: IOV data can be visualized using charts and graphs that show the exchange rates or transaction volumes between different blockchain networks or cryptocurrencies. Smart contract visualizations can be represented using various diagrams, such as flowcharts or state transition diagrams.Heat maps: Heat maps can be used to show the spatial or temporal distribution of transactions or trust scores.

3.4. Implementation of Modules:

Trust Metrics: Trust metrics are used to quantify the trustworthiness of nodes within the system. These metrics can be based on a variety of factors, such as the node's reputation, past behavior, and transaction history.Smart Contracts: Smart contracts are used to manage trust relationships between nodes within the system. These contracts are self-executing and enforceable, and they can be used to automatically initiate transactions based on predefined conditions.Trust Scores: Trust scores are assigned to nodes based on their trust metrics. These scores are used to determine the level of trustworthiness of each node within the system.Trust Updates: Trust scores are updated in real-time based on the behavior of nodes within the system. Nodes that exhibit trustworthy behavior will see their trust scores increase, while nodes that exhibit untrustworthy behavior will see their trust scores decrease.Adaptive Trust Management: The system uses adaptive trust management to dynamically adjust trust scores based on changing conditions within the system. This allows the system to quickly adapt to new threats and maintain a high level of security.

3.4.1 Network Formation :

In this module, we create a network consisting of nodes. Each node acts as a vehicle and has its own distance and range. We create nodes by giving latitude and longitude as input which in turn describes the vehicle location. Each node will be dynamic in position that is changing their position dynamically. We create ‘n’ number of nodes based on our requirement to form network environment or network formation.

3.4.2. Neighbour Calculation:

After network formation based on each node latitude and longitude neighbor calculation will be calculated. We calculate neighbor to send messages among nodes and communicate among them. Data will be sent to destination from source via neighbors if both source and destination are not within their communication range.

3.4.3. Emergency Event Occurred:

In VANET environment many emergency events can occur like for example Partial Brake, Emergency Brake, and Overtaking etc. When an emergency event occurs it create chaos in the environment. Based on the emergency event occurred an emergency message will be created.

3.4.4. Emergency Event Occurred:

After an emergency event occurred an emergency message will be created by the vehicle. Emergency message will be created based on the type of event occurred. Many emergency events may occur in the environment. For example events like sudden break, Partial Brake, Overtaking, ambulance takeover etc are some of the examples of the emergency event. If a vehicle detects a dangerous event, it immediately generates and broadcasts an emergency message to the vehicles in the region of interest (or target region with safety risks), such that the nearby vehicles can take effective actions to avoid traffic accident. In essence, the emergency message, which contains life-critical and time-sensitive information, should be disseminated to all targeted vehicles in a very efficient and effective way.

3.5 Deployment:

In this module the trained machine learning model is converted into pickle data format file (.pkl file) which is then deployed for providing better user interface and predicting the output of Human Stress and Deployment used here is Django Web Framework.
Django is a micro web framework written in Python.It is classified as a micro-framework because it does not require particular tools or libraries.

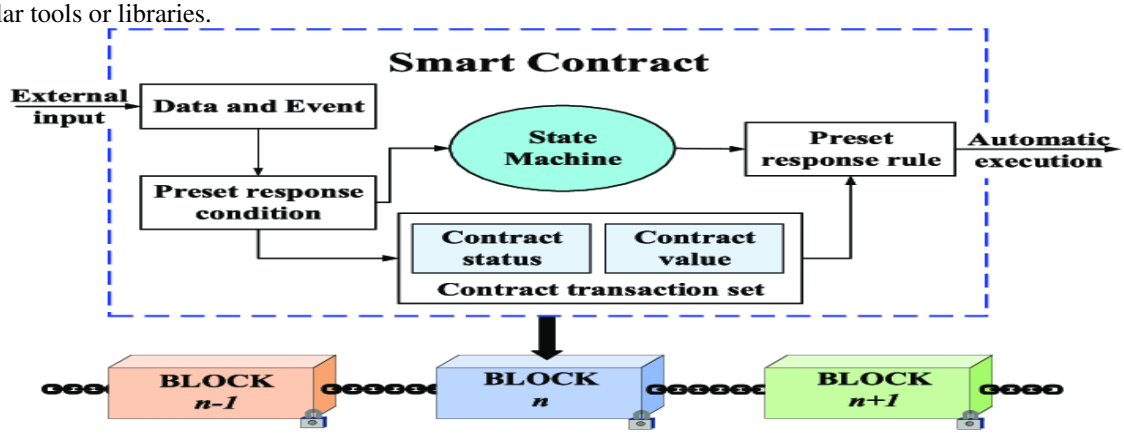

Figure 1 MODULE DIAGRAM

IV. EXPERIMENT RESULTS

Figure 2: User Login

Figure 3:Registration

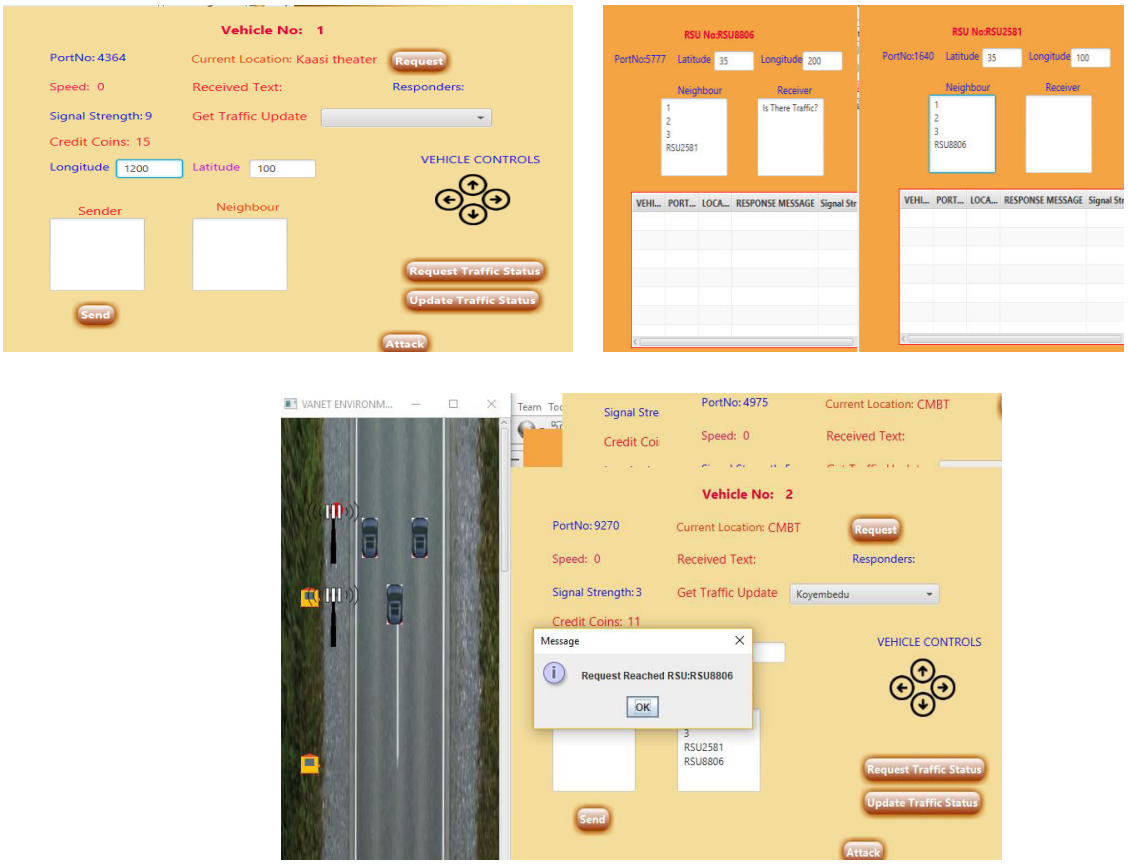

Figure 5: Output Screenshot

V. CONCLUSIONS

In conclusion, blockchain-based adaptive trust management using the IoV of smart contracts is a powerful tool for managing trust in a decentralized manner. This system uses trust metrics, smart contracts, trust scores, and adaptive trust management to ensure that nodes within the system are trustworthy and secure. Trust metrics are used to quantify the trustworthiness of nodes, while smart contracts are used to manage trust relationships between nodes. Adaptive trust management allows the system to dynamically adjust trust scores based on changing conditions, providing an additional layer of security.Overall, blockchain-based adaptive trust management using the IoV of smart contracts has the potential to revolutionize trust management in a variety of applications. By providing a decentralized, transparent, and secure system, this technology can help ensure the integrity of transactions and increase the overall level of trust in a wide range of industries.

REFERENCES

[1] T. A. Butt, R. Iqbal, S. C. Shah, and T. Umar, "Social Internet of Vehicles: Architecture and enabling technologies," *Comput. Elect. Eng.*, vol. 69, pp. 68–84, Jul. 2018.
[2] K. Z. Ghafoor, M. A. Mohammed, J. Lloret, K. A. Bakar, and Z. M. Zainuddin, "Routing protocols in vehicular ad hoc networks: Survey and research challenges," *Netw. Protocols Algorithms*, vol. 5, no. 4, pp. 39–83, 2013.
[3] J. Lloret, A. Canovas, A. Catalá, and M. Garcia, "Group-based protocol and mobility model for VANETs to offer Internet access," *J. Netw.Comput. Appl.*, vol. 36, no. 3, pp. 1027–1038, 2013.
[4] I. García-Magariño, G. Palacios-Navarro, R. Lacuesta, and J. Lloret, "ABSCEV: An agent-based simulation framework about smart transportation for reducing waiting times in charging electric vehicles,"
Comput. Netw., vol. 138, pp. 119–135, Jun. 2018.
[5] L. Guo *et al.*, "A secure mechanism for big data collection in large scale
Internet of Vehicle," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 601–610,
Apr. 2017.

[6] H.-T. Wu and G.-J. Horng, "Establishing an intelligent transportation system with a network security mechanism in an Internet of Vehicle environment," *IEEE Access*, vol. 5, pp. 19239–19247, 2017.
[7] N. Torabi and B. S. Ghahfarokhi, "Survey of medium access control schemes for inter-vehicle communications," *Comput. Elect. Eng.*, vol. 64, pp. 450–472, Nov. 2017.
[8] R. Bauza and J. Gozálvez, "Traffic congestion detection in large-scale scenarios using vehicle-to-vehicle communications," *J. Netw. Comput.Appl.*, vol. 36, no. 5, pp. 1295–1307, 2013.
[9] A. Aliedani and S. W. Loke, "Cooperative car parking using vehicle-to-vehicle communication: An agent-based analysis," *Comput. Environ. Urban Syst.*, Jun. 2018. [Online]. Available: https://doi.org/10.1016/j.compenvurbsys.2018.06.002
[10] M. Wang, "Infrastructure assisted adaptive driving to stabilise heterogeneous vehicle strings," *Transp. Res. C Emerg. Technol.*, vol. 91, pp. 276–295, Jun. 2018.
[11] K. Z. Ghafoor, K. A. Bakar, J. Lloret, R. H. Khokhar, and K. C. Lee, "Intelligent beaconless geographical forwarding for urban vehicular environments," *Wireless Netw.*, vol. 19, no. 3, pp. 345–362, 2013.
[12] G. De La Torre, P. Rad, and K.-K. R. Choo, "Driverless vehicle security: Challenges and future research opportunities," *Future Gener. Comput. Syst.*, Jan. 2018. [Online]. Available: https://doi.org/10.1016/j.future.2017.12.041
[13] A. Fernández-Isabel and R. Fuentes-Fernández, "Analysis of intelligent transportation systems using model-driven simulations," *Sensors*, vol. 15, no. 6, pp. 14116–14141, 2015.
[14] S. Harrabi, I. B. Jaafar, and K. Ghedira, "A novel clustering algorithm based on agent technology for VANET," *Netw. Protocols Algorithms*, vol. 8, no. 2, pp. 1–19, 2016.
[15] K. Grover, A. Lim, S. Lee, and Q. Yang, "Privacy-enabled probabilistic verification in broadcast authentication for vehicular networks," *Ad HocSensor Wireless Netw.*, vol. 32, nos. 3–4, pp. 239–274, 2016
[16] W. I. Khedr, "Improved lightweight authentication scheme for IEEE
802.11p vehicle-to-infrastructure communication," *Ad Hoc Sensor*

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |

www.ijarasem.com