JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

AN EFFECTIVE PRIVACY-PRESERVING HANDOVER AUTHENTICATION SCHEME FOR THE INTERNET OF VEHICLES BASED ON BLOCKCHAINS

[1]Dr. SOUNDER J,[2]Ms. QUEENKIRUBAANANTHY S,[3]Ms. SHARMILA S, [4] Dr. CHITRA

[1] *Head of the Department, Department of Electronics and Communication System, Cheran's Arts Science College, Kangeyam, TN, India.*

[2] *Founder and Developer, GTS Research Academy Pvt Ltd, Salem, TN, India.*

[3] *Assistant Professor, Department of Computer Applications and Information Technology, Kaamadhenu Arts and Science College, Sathyamangalam, TN, India.*

[4] *Assistant Professor, Department of computer Science, Government Arts College (Autonomous), Salem, TN, India.*

Abstract: The Internet of Vehicles (IoV) can greatly increase the effectiveness of transportation systems and guarantee traffic safety. A fundamental line of defense against attacks in IoV is authentication. However, cutting-edge methods have several problems, such as leakage of vehicle trajectory confidentially, bottlenecks of a single cloud server architecture, significant computing overhead of operations, and an excessive reliance on cloud servers and roadside units (RSUs). To solve these issues, BEPHAP, an effective privacy-preserving handover authentication mechanism based on blockchains, as well as the Internet of Vehicles' flagship protocol, are presented in this study. With key protocols based on tamper-proof blockchains, symmetric cryptography, and chameleon hash functions and a security paradigm that supports cloud server and RSU assaults, BEPHAP achieves anonymous cross-domain mutual handover authentication. BEPHAP is especially well suited for IoV since it restricts vehicle activity to minimal cryptographic operations during the authentication stage. Data confidentiality, unlinkability, traceability, non-repudiation, non-frame capability, and key escrow freedom are also attained by BEPHAP. Formal security proofs based on BAN logic and formal verification based on ProVerif show that BEPHAP is resistant to a variety of targeted assaults, including man-in-the-middle, impersonation, and replay attacks. According to the performance analysis, BEPHAP performs better than other functions in terms of computing and communication. At 5000 requests per second, the message rate is not lost, which satisfies the IoV criteria.

IndexTerms **- Internet of vehicles, handover authentication,blockchain, privacy-preserving, BAN logic, ProVerif.**

I. INTRODUCTION

The Internet of Vehicles (IoV), a crucial component of Intelligent Transportation Systems (ITS), can considerably increase the effectiveness of transportation while lowering energy consumption and traffic accidents. Infrastructure includes items along the road. Cloud servers are in charge of providing services to vehicles, and roadside units can be used for communication between vehicles and cloud servers. Roadside units can be utilized as edge servers for vehicles to connect with. thought through. In these networks, automobiles can communicate with other participants in real-time traffic information such as position, speed, and traffic congestion. Reliable authentication methods are crucial for supporting information dissemination securely and efficiently. In an authentication method, two parties a vehicle and an RSU—can confirm the legitimacy of the other party through a series of message exchanges through an unprotected communication channel. However, IoV faces many difficulties:

1) Adversaries that conduct privacy mining and data association in massive real-time message distribution of IoV can protect user privacy. Adopting pseudonymous procedures to safeguard real identities is a logical solution to privacy problems.
2) Because IoV is open, it is susceptible to some security risks, including man-in-the-middle attacks, impersonation attacks, eavesdropping attacks, and specific replay attacks.
3) The majority of the current Internet of Vehicles (IoV) solutions use a centralized structure, which means that all vehicles can only authenticate to the cloud server and that RSU can only be used as an intermediary node to facilitate communication between the vehicle and the cloud server.

OBJECTIVE

The proposed solution to the aforementioned issues is BEPHAP, a blockchain-based effective privacy-preserving handover authentication protocol with the IoV's flagship protocol. Blockchain is ideally suited to address cross-domain authentication issues in a multi-cloud scenario since it is a distributed peer-to-peer network. Blockchain is utilized in BEPHAP to synchronize vehicle-related data across each cloud server and make it possible for them to cooperatively manage vehicle data across the network. No adversary, including cloud servers and RSUs, can readily tamper with vehicle-related information recorded in the blockchain due to the blockchain's tamper-proof feature.

HYPOTHESIS

1) BEPHAP is the first blockchain-based authentication protocol scheme for the Internet of Values (IoV) that enables mutual authentication with concurrent key agreement, data privacy, identity anonymity, unlinkability, traceability, non-repudiation, and non-flammability. verification using formal security verification methods, cross-domain formal security proofs, and key escrow freeness.

2) For Internet of Vehicles scenarios with constrained vehicle computing capabilities, a novel low-latency authentication approach is suggested. Because BEPHAP restricts vehicle authentication to simple cryptographic processes like hashing and symmetric encryption.

3) We take into account a security framework that allows both cloud servers and RSUs to launch attacks. According to the security model, the security evaluation demonstrates that BEPHAP can offer conditional privacy protection and stop any organization, including cloud servers or RSUs, from producing honest cars.

4) It is demonstrated, using BAN logic and ProVerif formal security verification tools, that our protocol has unique security properties.

II. RELATED WORKS

Seo et al (2018) have declared that the acknowledgment of range detection is turning out to be more also, more conceivable with the advancement of advances, for example, man-made consciousness and programming radio. While it has to pay regard to its presentation, it can't overlook the security issues it faces. It has been proposed an advancement plan to guard against range-detecting data adulteration (SSDF) assaults in light of the twofold limit energy discovery and square chain innovation [1].

Puppala et al (2016) have uncovered that the medical care administration industry is consistently giving indications of progress and supporting new headways and progresses. One of the transcendent necessities in the present medical care frameworks is to secure the patient's clinical report against likely aggressors. Subsequently, it is fundamental to have secured data that can simply support individuals can get to the patient's clinical report [2].

Tranieri et al (2013) have point by point that Cardiovascular autonomic neuropathy (CAN), one of the significant confusions in diabetes, whenever recognized at the subclinical stage takes into account viable treatment and stays away from additional complexity including cardiovascular pathology. Surface ECG (Electrocardiogram)- based conclusion of CAN is helpful to defeat the restriction of existing cardiovascular autonomic reflex tests customarily utilized for CAN distinguishing proof in clinical settings [3].

Victoria et al (2016) have declared that a ton of archives are kept up by mediators just to guarantee the legitimacy and uprightness of the archives. There is a ton of assets put in for upkeep reasons yet the vast majority of the time the framework neglects to convey what is guaranteed. With the approach of Blockchain innovation, it can help specialists to keep up with it [4].

Mohamed Tahar et al (2018) have uncovered that the IoT plays a critical part in our each day timetable and it incredibly influences us. Central security objectives like classification, respectability and accessibility are significant difficulties in IoT because of their distributive nature and monstrous scale. The decentralized methodology utilized in BC would make a more dependable framework for gadgets, to run on by killing weak links. Diverse cryptographic calculations utilized in blockchains, would bring about more noteworthy security of purchaser data [5].

Zhonglin Chen et al (2018) point by point that the super thick organization (UDN) is perhaps the most encouraging advancement in the fifth era (5G) to address the network framework limit issue. In any case, it is another test that the client equipment（UE） secure access UDN made out of the passageways (APs) which are described as self-rule, impermanent and dynamic. In 5G UDN, the APS is autonomous and equivalent. The UDN can be viewed as a decentralized admittance organization [6].

Tipping et al (2011) have declared that the RVM empowers meager characterization and relapse capacities to be gotten by directly weighing a few fixed premise capacities from a huge word reference of potential candidates.TOA on RVM has O(M3) time and O(M2) space intricacy, where M is the preparing set size. It is accordingly computationally infeasible on exceptionally enormous data collections which are proposed CBA [7].

Simon Fraser et al (2014) has uncovered that the utilization of computerized applications is on the ascent these days. So the preparation of that data is finished by a device called MapReduce. MapReduce has a construction that can't be adjusted. While preparing that data, the slant will happen in both guides and lessen the stage. Guide slant is not difficult to diminish yet, if there should arise an occurrence of decreased stage it might require some investment to diminish it [8].

Satoshi Nakamoto et al (2017) have pointed the point that the Production network Management frameworks give data sharing and investigation to organizations and back their arranging exercises. They are not founded on genuine data because there is lopsided data between organizations, then, at that point driving to aggravation of the arranging calculations [9].

Marzouki et al (2017) has declared that the research has proposed another encoding strategy roused from the square chain innovation, by which an activity arrangement data and the comparing machine data are incorporated in an activity hub and connections all activity hubs to frame an activity list with pointer innovation of C++ program language [10].
Manikandan D, Valliyammai C, Karthika RN (2020) et.al decide on the security handling to assist with working on the data in the blockchain of the digital currency and time. It forestalls data altering, and confirmation issues while getting to the unified

workers. It helps to zero in on distributed storage and the executives for security-improving by sidestepping the malignant clients. By utilizing the SWOT (Strengths Weakness Opportunities Threats) investigation to perform and tend to the benefits and innovation advancements in blockchain calculation [11].

S. Dhanalakshmi, G.Charles Babu (2019) et.al portrays the bitcoin innovation for crypto-currency exchanges in digitized, decentralized, trusted, and got in circulated record. Each exchange has been confirmed by the hashing algorithm alongside a gigantic measure of data. It covers the defects of capacity in digital money and gives the elements of the condition of the cycle, attributes, and applications associated with enormous data investigation while utilizing the BlockChain calculation [12]. It assists with working on the connection between digital money, security, and adaptability to decentralization alongside straightforwardness. Besides, it has been displayed as a huge data insightful structure to find the cycle of bitcoins.

Alex. R. Mathew (2019) et.al portray the digital money adjust to businesses, finance, and so on To find the cycle alongside digital protection by utilizing Blockchain methods in huge data. To examines this advancement under 30 scientists. Blockchain algorithms along with IoT, Networks, and data discriminate the versatility and improve the efficiency in security management. The solutions from uniformity while examining the existing and proposed techniques in the future [13].

Dong Wang, Huanjuan Wang, and Yuchen Fu (2021) et.al depict the security of the slat and controlling ability in huge data while examining the working progress alongside the IoT and brilliant network. It joins to give a gigantic response while getting to the 5G MEC at the edge of the 5G organization framework. It gives dependability and precision by utilizing blockchain calculation. It sent the MEC entryway/Server. It concentrates to recognize the weaknesses by utilizing PoW, PoS, DPoS, and PDFT to play out the distinctive agreement of normal registering time and understanding point of view [14].

Swagatika Sahoo, Rishu Roshan, Vikash Singh, and Raju Halder are still up in the air business development as the main thrust and increment the adaptation of the promoting field the other way around. Yet, the dangers that have happened while entering the data-driven situation convey inclined to different intimidations. It was overwhelmed by utilizing the BDmarks of watermarking to build the adaptation and stay away from the dangers inside and outside, increment the security products for business development [15].

III. METHODOLOGY

3.1 Law Enforcement Authority (LEA):

An authorized legal entity (LEA) that is capable of identifying malicious vehicles for network audits should exist. The only agency that has the power to divulge a hostile vehicle's real identity is LEA. A complete blockchain node can be deployed on LEA, allowing it to contribute registration data to the blockchain, and it has significant computing and storage resources. The actual identities of vehicles and registration information are managed by LEA.

3.2 Regional Service Manager (RSM):

The LEA has given RSM, in the form of cloud-based servers with powerful computing and storage capacity, the authority to handle car registration, certification, and cancellation. Each of the numerous domains that make up the overall network has an RSM in charge of maintaining the vehicles in that domain. acts as a full node in each RSM Blockchain network, storing data on car cancellation, registration, and authentication. RSM is required to report the trajectory of harmful vehicles in your domain to LEA in addition to the following penalize or track malicious vehicles. To connect several communications from hostile vehicles, RSM needs this capability.

3.4 Roadside Unit (RSU):

To manage and coordinate vehicle communication, RSUs are widely dispersed throughout the highways. Calculation and storage RSU's capacity is less robust than RSM's. Although the hardware is still being developed, RSU still has enough computational and storage power to help with some of the workloads throughout the certification process, lowering the administrative burden on RSM. Additionally, RSU is required to report and track the trajectory of malicious cars in your service area to RSM to penalize or track hostile vehicles. RSU is hence referred to as multiple. Messages from the hostile vehicle must be able to connect.

3.5 On-board Unit (OBU):

OBU is an onboard computing and communication device with a constrained amount of storage and transmission space. A vehicle with an OBU can communicate with neighboring RSUs, infrastructure, or other cars.

3.6 Fog Saver (FS):

Messages between RSM and RSU are forwarded by FS, which has fewer computing and storage resources than RSM. Vehicles frequently travel over a vast area and may cross into several distinct regions. In actuality, the deployment of authentication servers, the type of network access, and the number of access points vary widely among regions. For instance, RSM is used in various areas. Between RSU, there are some fog servers, however, there are some locations without any.

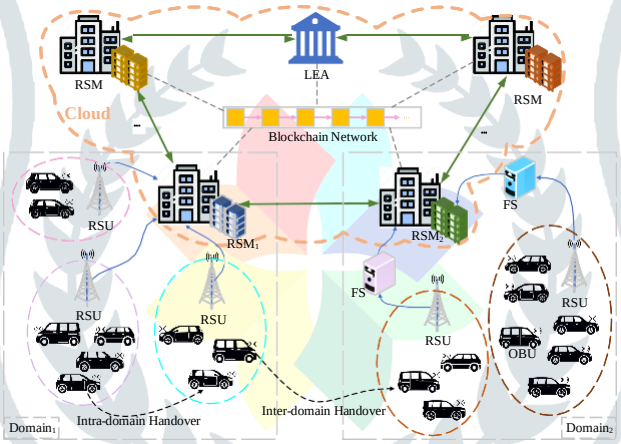

Fig -1: System Architecture

IV CONCLUSION AND FUTURE ENHANCEMENT

To introduce the BEPHAP protocol for the Internet of Things (IoV) under a security architecture that allows attacks from cloud servers and RSUs. BEPHAP is a blockchain-based efficient privacy-preserving handover authentication mechanism with a Key Agreement. We can create cross-domain privacy-preserving handover authentication using blockchain, symmetric cryptography, and chameleon hashes. We believe BEPHAP to be the first blockchain-based authentication protocol scheme for IoV that simultaneously provides key agreement, data privacy, identity anonymity, anonymity, traceability, non-repudiation, non-flammability, and mutual with key escrow. Carries out authentication. Verification using formal security verification techniques, formal security proofs, cross-domain verification, and independence. Because only simple cryptographic operations, including symmetric encryption and hashing, are needed from the vehicles during the authentication phase, BEPHAP is especially well suited for IoV scenarios with limited vehicle computing capabilities. An individual RSU may respond to an authentication request in 0.2 milliseconds, which is faster than existing techniques, according to experiments. It's also important to note that BEPHAP reduces the computational cost of VN by two to three orders of magnitude compared to other techniques.

REFERENCES

[1] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," in Proceedings of the Twelfth ACM Symposium on Operating System Principles, SOSP 1989, The Wigwam, Litchfield Park, Arizona, USA, December 3-6, 1989, G. R. Andrews,

Ed. ACM, 1989, pp. 1–13. [Online]. Available: https://doi.org/10.1145/74850.74852.

[2] B. Blanchet, B. Smyth, V. Cheval, and M. Sylvestre, "Proverif 2.00: automatic cryptographic protocol verifier, user manual and tutorial,"Version from, pp. 05–16, 2018.

[3] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in Q2SWinet'05 - Proceedings of the First ACM Workshop on Q2S and Security for Wireless and Mobile Networks, Montreal, Quebec, Canada, October 13, 2005, A. Boukerche and R. B. de Araujo, Eds. ACM, 2005, pp. 79–87. [Online]. Available: https://doi.org/10.1145/1089761.1089775.

[4] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of computer security, vol. 15, no. 1, pp. 39–68, 2007.

[5] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," in INFOCOM 2008. 27th IEEE International Conference on ComputerCommunications, Joint Conference of the IEEE Computer and Communications Societies, 13-18 April 2008, Phoenix, AZ, USA.

[6] Seo.D and Nam.H., "A parallel multi-channel cooperative spectrum sensing in cognitive radio networks," 2018 International Symposium on Antennas and Propagation, Busan, Korea (South), 2018, pp. 1-2.

[7] Puppala.M, He.T, Yu. X, Chen.S, Ogunti. R, and Wong. S.T.C, "Data security and privacy management in healthcare applications and clinical data warehouse environment," in 2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI), Feb 2016, pp. 5–8.

[8] Stranieri. A Abawajy. J, Kelarev. A Huda.S, Chowdhury.M, and Jelinek. H.F, ''An approach for Ewing test selection to support the clinical assessment of cardiac autonomic neuropathy,'' Artif. Intell. Med., vol. 58, no. 3, pp. 185–193, Jul. 2013.

[9] Victoria. L, Lemieux, 'Trusting records: is Blockchain technology the answer? Records Management Journal' 26(2):2016, pp. 110-139.

[10] Hammi, Mohamed Tahar, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT." Computers & Security 78 (2018): 126-142.

[11] Zhonglin Chen, Shanzhi Chen, Hui Xu, Bo Hu, "A Security Scheme of 5G Ultra-Dense Network Based on Implicit Certificate," Wireless Communications and Mobile Computing, vol. 2018, no. 11, 23 May.2018.

[12] Tipping. M.E., Sparse Bayesian learning, and the relevance vector machine. Journal of Machine Learning Research, 1:211–244, 2011.

[13] Yanfang Le; Simon Fraser Univ., Burnaby, BC, Canada; Jiangchuan Liu; Ergun, F.; Dan Wang, "Online Load Balancing for MapReduce with Skewed Data Input" IEEE, pg 2004 - 2012.,2014.

[14] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf [Accessed March 2017].

[15] Marzouki. B, Driss. O.B, Ghdira. K, Multi-Agent model based on Chemical Reaction Optimization with Greedy algorithm for Flexible Job shop Scheduling Problem, Procedia ComputerScience 112 (2017) 81–90.

[16] Manikandan D, Valliyammai C, Karthika RN, Blockchain-based Secure Big Data Storage on Cloud, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-9 Issue-4, November 2020.

[17] S. Dhanalakshmi, G.Charles Babu, An Examination Of Big Data And Blockchain Technology, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-11, September 2019.

[18] Alex. R. Mathew, Cyber Security through Blockchain Technology, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-1, October 2019.

[19] Dong Wang, Huanjuan Wang & Yuchen Fu, Blockchain-based IoT device identification and management in 5G smart grid, EURASIP Journal on Wireless Communications and Networking volume 2021, Article number: 125 (2021).

[20] Swagatika Sahoo, Rishu Roshan, Vikash Singh, and Raju Halder, BDmark: A Blockchain-driven Approach to Big Data Watermarking, ACIIDS, 2020