IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 2, February 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302061 |

Blockchain-Based Secret Key Extraction for Efficient and Secure Authentication in VANETs

Pravin.N, Mr.S.Jagadeesan M.E, Dr.P.Sukumar M.E.,Ph.D, Mrs.N.M.Indumathi M.E, Mrs.Padma M.Tech, Ms.M.Deepika M.E

PG Scholar, Department of CSE, Nandha Engineering College (Autonomus), Erode, Tamil Nadu, India

Assistant Professor, Department of CSE, Nandha Engineering College (Autonomus), Erode, Tamil Nadu, India

Professor, Department of CSE, Nandha Engineering College (Autonomus), Erode, Tamil Nadu, India

Assistant Professor, Department of CSE, Nandha Engineering College (Autonomus), Erode, Tamil Nadu, India

Assistant Professor, Department of CSE, Nandha Engineering College (Autonomus), Erode, Tamil Nadu, India

Assistant Professor, Department of CSE, Nandha Engineering College (Autonomus), Erode, Tamil Nadu, India

ABSTRACT*:* We have developed a blockchain-based trust management model for preserving location privacy in Vehicular Impromptu Networks (VANETs), a crucial component of Intelligent Traffic Systems (ITS). VANETs offer high mobility, but security concerns have remained unresolved, especially when leveraging Location-Based Services (LBS). Our solution enables vehicles to request LBS using authentication without disclosing their private information. We establish anonymous shrouding zones to ensure vehicle privacy, employ a algorithm to regulate vehicle behavior, and utilize blockchain technology to enhance data security. Through extensive testing, we have demonstrated the system's resilience to various trust model attacks, effectively safeguarding vehicle privacy. Simulation results further confirm the viability and effectiveness of our proposed system in real-world scenarios.

KEYWORDS: Ad Hoc Networks, Blockchain, KeyDer, Vanets.

I. INTRODUCTION

The emergence of Vehicular Ad Hoc Networks (VANETs) has ushered in a new era of enhanced connectivity and data exchange among vehicles and roadside infrastructure, promising revolutionary advancements in road safety, traffic management, and transportation efficiency. However, this heightened interconnectivity necessitates robust security and privacy measures to protect the sensitive information transmitted within these networks. To address these concerns, an innovative solution has arisen: the Efficient Blockchain-based Conditional Privacy-preserving Authentication for VANETs. This groundbreaking concept leverages blockchain technology and advanced cryptographic techniques to strike a delicate balance between authentication and privacy, enabling vehicles to securely prove their identities while safeguarding their sensitive data. This exploration delves into the concept's key components and benefits, highlighting its potential to revolutionize the landscape of VANET security and privacy.

II. LITERATURE SURVEY

A. SECURE AND LIGHTWEIGHT CONDITIONAL PRIVACY-PRESERVING AUTHENTICATION FOR SECURING TRAFFIC EMERGENCY MESSAGES IN VANETS

In their paper, Lu Wei and colleagues address the growing importance of Vehicular Ad Hoc Networks (VANETs) in enhancing traffic safety and driving convenience due to advancements in wireless communication technology and the increasing number of automobiles. They identify the need for a Conditional Privacy-Preserving Authentication (CPPA) scheme in VANETs, given their vulnerability and security requirements. Traditional CPPA schemes suffer from two shortcomings: insufficiently low communication/storage overhead for ultra-low transmission delay requirements of traffic emergency messages and neglect of system secret key (SSK) updates stored in tamper-proof devices, increasing the risk of SSK breaches.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302061 |

AN ENERGY-EFFICIENT DATA FORWARDING STRATEGY FOR HETEROGENEOUS WBANS

In their paper, Dapeng Wu et al. introduce an energy-efficient data forwarding strategy (EDFS) aimed at addressing critical challenges in Wireless Body Area Networks (WBANs), particularly in the context of healthcare applications. These networks rely on body sensors with limited energy resources, making efficient energy management crucial to mitigate performance issues like latency and energy efficiency degradation. EDFS employs compressed sensing to reduce the size of transmitted physiological data and optimizes relay sensor selection by considering factors such as remaining energy levels, sampling frequency, and sensor importance. This approach enhances energy efficiency and network reliability while effectively adapting to dynamic WBAN topologies.

B. TFPPASV: A THREE-FACTOR PRIVACY PRESERVING AUTHENTICATION SCHEME FOR VANET

Duan et al. emphasize the critical role of Vehicular Ad Hoc Networks (VANETs) in the autonomous vehicle industry, highlighting the escalating security threats accompanying advancements in VANET technology. They identify vulnerabilities in Xu et al.'s three-factor (3F) authentication scheme, revealing its susceptibility to dishonest Roadside Units (RSUs) bypassing the Trusted Authority (TA) and initiating unauthorized sessions with On-Board Units (OBUs). In response, Duan et al. propose a novel 3F authentication scheme called TFPPASV, designed to thwart RSU attempts at bypassing the TA while safeguarding user privacy.

C. BCPPA: A BLOCKCHAIN-BASED CONDITIONAL PRIVACY-PRESERVING AUTHENTICATION PROTOCOL FOR VEHICULAR AD HOC NETWORKS

In their system, Chao Lin et al. address the challenges of security and privacy in Vehicular Ad-hoc Networks (VANETs), which have the potential to enhance driver safety and traffic management efficiency through real-time traffic information sharing among vehicles. They highlight the limitations of existing conditional privacy-preserving authentication (CPPA) protocols, particularly in the context of VANET deployment. To tackle these issues, the authors propose a novel blockchain-based CPPA (BCPPA) protocol, leveraging Ethereum as a public blockchain, to facilitate secure communication in VANETs.

D. PA-CRT: CHINESE REMAINDER THEOREM BASED CONDITIONAL PRIVACY-PRESERVING AUTHENTICATION SCHEME IN VEHICULAR AD-HOC NETWORKS

In their system, Jing Zhang et al. have introduced an innovative approach to enhancing security and privacy in Vehicular Ad-hoc Networks (VANETs) by addressing the limitations of existing identity-based vehicular communication protocols. Unlike conventional methods reliant on tamper-proof devices (TPDs), this novel protocol leverages the Chinese remainder theorem (CRT) to achieve conditional privacy-preserving authentication without the need for pre-loaded master keys on vehicles' TPDs.

E. A TRACEABLE BLOCKCHAIN-BASED ACCESS AUTHENTICATION SYSTEM WITH PRIVACY PRESERVATION IN VANETS

Dong Zheng et.al. Has proposed in this paper as of late, The vehicular specially appointed networks (VANETs) is one of the most encouraging application in the correspondences of savvy vehicles and the shrewd transportation frameworks. In any case, confirmation and security of clients are as yet two essential issues in VANETs. It is urgent to keep inward vehicles from broadcasting the fashioned messages while safeguarding the security of vehicles against the following assault. Also, in the customary mode, the value-based information capacity gives no dispersed and decentralized security, with the goal that the outsider starts the untrustworthy ways of behaving potentially.

F. BPAS: BLOCKCHAIN-ASSISTED PRIVACY-PRESERVING AUTHENTICATION SYSTEM FOR VEHICULAR AD-HOC NETWORKS

In this paper, Qi Feng et al. propose that the establishment of a wireless communication channel connecting all vehicles can enable vehicular ad-hoc networks (VANETs) to support a wide range of real-time traffic information services, including intelligent routing, weather monitoring, and emergency calls. However, the accuracy and credibility of the messages transmitted among VANETs are of paramount importance, as human life may depend on them. To address this issue, we introduce a novel framework called the blockchain-assisted privacy-preserving authentication system (BPAS), which provides automatic authentication in VANETs while preserving vehicle privacy.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302061 |

G. EXTENSIBLE CONDITIONAL PRIVACY PROTECTION AUTHENTICATION SCHEME FOR SECURE VEHICULAR NETWORKS IN A MULTI-CLOUD ENVIRONMENT

Jie Cui Et.al. Has proposed in this paper with a rising number of cloud specialist organizations (CSPs), research chips away at multi-cloud conditions to give answers for stay away from seller secure and manage the single-point disappointment issue have extended extensively. In any case, a couple of plans center around the restrictive security confirmation of vehicular organizations under a multi-cloud climate. In such manner, we propose a hearty and extensible verification plot for vehicular organizations to satisfy the evergrowing broadened administration requests from clients. As indicated by our answer, the vehicles need to enroll with the confided in power (TA) just a single time to accomplish a quick and proficient verification with CSPs.

H. BLOCKCHAIN FOR INTERNET OF THINGS: A SURVEY

Hong-Ning Dai et.al. Has proposed in this paper Web of Things (IoT) is reshaping the occupant business to brilliant industry highlighted with information driven decision making. Notwithstanding, natural highlights of IoT bring about various difficulties like decentralization, unfortunate interoperability, and protection and security weaknesses. Blockchain innovation acquires the amazing open doors tending to the difficulties of IoT. In this paper, we explore the joining of blockchain innovation with IoT. We name such blend of blockchain and IoT as Blockchain of Things (BCoT). This paper presents an inside and out study of BCoT and examines the bits of knowledge of this new worldview. Specifically, we first momentarily present IoT and examine the difficulties of IoT. Then, at that point, we give an outline of blockchain innovation.

I. WIDEBAND MILLIMETER-WAVE PROPAGATION MEASUREMENTS AND CHANNEL MODELS FOR FUTURE WIRELESS COMMUNICATION SYSTEM DESIGN

Theodore S et.al. Has been proposed this paper the generally unused millimeter-wave (mmWave) range offers astounding chances to increment versatile limit due to the huge measure of accessible crude data transmission. This paper presents trial estimations and observationally based engendering channel models for the 28, 38, 60, and 73 GHz mmWave groups, utilizing a wideband sliding connect channel sounder with steerable directional horn receiving wires at both the transmitter and recipient from 2011 to 2013. In excess of 15,000 power postpone profiles were estimated across the mmWave groups to yield directional and omnidirectional way misfortune models, fleeting and spatial channel models, and blackout probabilities

J. VEHICULAR CLOUD COMPUTING: ARCHITECTURES, APPLICATIONS, AND MOBILITY

Azzedine Boukerche, Robson E. De Grande et.al.,has proposed Shrewd transportation systems are expected to give inventive applications and organizations relating to traffic the board, similarly as to work with the induction to information for various structures and clients. The persuading motivation for using underutilized locally accessible resources for transportation structures and the degrees of progress in organization development for Cloud figuring resources has progressed the possibility of Vehicular Mists. This work gathers and depicts the most recent strategies and deals with Vehicular Mists, including applications, organizations, and traffic models that can engage Vehicular Cloud in an all the more remarkable environment.

K. A FIRST LOOK AT IDENTITY MANAGEMENT SCHEMES ON THE BLOCKCHAIN

Paul Dunphy and Fabien A.P. Petitcolas et.al,has proposed 24 years have passed since Peter Steiner initially showed the world that "on the Web, nobody knows no doubt about it," yet that praised drawing in still stands to address the test to perceive individuals on the web. Today, we are far from the public library vision of the creators of public-key cryptography during the 1970s or the well conceived plan of moderate affirmation envisioned during the 1980s. Character the board (IdM) on the Web really relies upon what Cameron considered 10 years earlier a "joined of character one-offs,"1 including a couple of sorts of IdM systems that are restricted to express spaces and don't team up much with one another.

L. BLOCKCHAIN TECHNOLOGIES FOR THE INTERNET OF THINGS: RESEARCH ISSUES AND CHALLENGES

Mohamed Amine Ferrag, Makhlouf Derdour et.al,has proposed This paper presents a total outline of the current blockchain shows for the Web of Things (IoT) associations. We start by portraying the blockchains and summarizing the ongoing investigations that oversee blockchain headways. By then, we give a diagram of the application spaces of blockchain propels in IoT, e.g, Web of Vehicles, Web of Energy, Web of Cloud, Haze enlisting, etc Likewise, we provide a request for peril models, which are considered by blockchain shows in IoT associations, into five rule classes, to be explicit, character based attack.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302061 |

M. PRIVACY-PRESERVING USER IDENTITY IN IDENTITY-AS-A-SERVICE

Tri Hoang Vo, et.al, has proposed Woldemar Fuhrmann In Unified Character The board, providers from different security spaces exchange messages containing approval and authorisation accreditations of clients. Consequently, a client can use his Own Recognizable Data (PII) from no less than one Character Suppliers to get to various districts. Scattering PII over delegates also requires safeguarding PII from being manhandled and unapproved access. Lifestyle as-aService (IDaaS) gives a unified person to clients to get to various Cloud organizations on demand yet may shield client insurance. In this paper, we present a clever philosophy for safeguarding security in IDaaS by combining Reason Based Admittance Control and Trait based Encryption with multi-experts support.

N. A SURVEY ON BLOCKCHAIN-BASED IDENTITY MANAGEMENT SYSTEMS FOR THE INTERNET OF THINGS

Xiaoyang Zhu et.al,has proposed The Web of Things targets partner everything going from individuals, affiliations, associations to things in the physical and virtual world. The automated character has reliably been considered as the foundation for each internet based help and the foundation for building security instruments like confirmation and endorsement. In any case, recurring pattern composing really unlucky deficiencies of a total investigation on the high level person the board for the Web of Things (IoT). In this paper, we separate high level character troubles and deals with the Web all things considered.

III. EXISTING SYSTEM

In this paper, we introduce a novel Blockchain-based Conditional Privacy-Preserving Authentication (BCPPA) solution tailored for Vehicular Ad-hoc Networks (VANETs), aiming to address the intricate balance between anonymity, traceability, and key/certificate management. Current BCPPA protocols have drawbacks, imposing substantial verification and traceability costs, which hinders their applicability in high-mobility, low-latency, and real-time VANET scenarios. To overcome these limitations, we propose three fundamental system components: KeyDer, Signatures of Knowledge (SoK), and a smart contract, culminating in an efficient BCPPA protocol named EBCPA. We demonstrate EBCPA's capability to meet essential requirements such as message authentication.

IV. PROPOSED SYSTEM

In order to enhance the performance of Wireless Sensor Networks (WSNs), we propose the Identity-Based Online/Offline Digital Signature (IBOOS) algorithm for secure data transmission in Cluster-based Wireless Sensor Networks (CWSN). Our goal is to achieve energy efficiency, and to this end, we introduce two novel Secure and Efficient Data Transmission (SET) protocols: IBOOS, which builds upon the Identity-Based Digital Signature (IBS) scheme, and an enhanced CP-ABE scheme based on Diffie-Hellman cryptography. These improvements streamline the architecture, reduce the involvement of trusted authorities, and minimize communication overhead between them and Virtual Controllers (VCs). We implement a central controller containing content server, RSU (ROAD SIDE UNIT), and vehicle details, allowing multiple control servers to be generated with RSUs, displaying available content server IDs in the respective RSUs. RSUs can connect to the content server as needed, and vehicle node details are displayed in the RSU interface. Additionally, data replication is facilitated within the vehicle when the nearest RSU is accessible, optimizing data management in this context.

A. ENCRYPTION MODULE

The proposed lightweight CP-ABE (Chipertext-Policy Attribute-Based Encryption) scheme for mobile cloud-assisted cyber-physical systems involves three key algorithms. The first algorithm is responsible for distributing public parameters and securely maintaining a master secret key for the entire system. The second algorithm, encryption, generates cipher text by utilizing the public parameters, input data, and access policy, which is subsequently transmitted to the cloud. Lastly, the decryption algorithm is responsible for retrieving the data from the cipher text using the master secret key and a set of attributes, ensuring that only users whose attributes satisfy the access policy can successfully decrypt the cipher text.

B. CENTRAL CONTROLLER SERVER

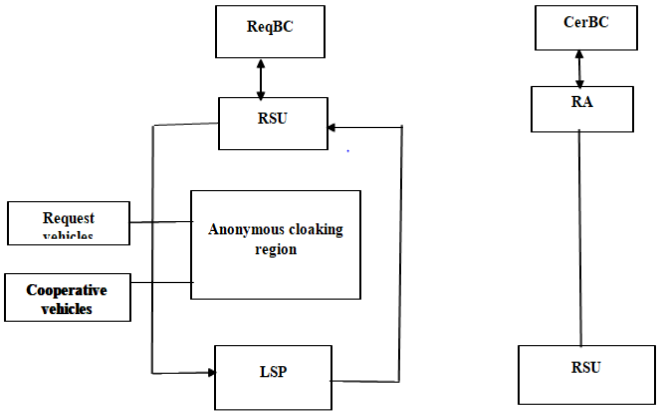
The central controller module serves as the central hub for managing RSU details, available content server IDs, and facilitating communication with the nearest vehicles through RSUs. Within this module, users can access and create RSU IDs and location IDs within the content server, while data replication in vehicles is also handled as part of the server's

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302061 |

functionality. The use of software-defined networks enables programmable configuration, allowing network administrators to script SDN programs for configuring, managing, securing, and optimizing network resources. This approach leverages open and VANET methods, ensuring freedom from server lock-in, much like the versatility seen in personal computers, regardless of the underlying hardware.



C. BI LINEAR PARING MODULE

This paper introduces an innovative approach to address the computational cost associated with bilinear pairings in pairing-based cryptographic protocols. Our proposal presents an efficient and secure outsourcing algorithm designed for execution within the two untrusted program model. A noteworthy feature of our algorithm, distinguishing it from existing state-of-the-art solutions, is its elimination of resource-intensive operations, such as point multiplications or exponentiations, for the outsourcer. Moreover, we leverage this algorithm as a crucial subroutine to enable outsource-secure identity-based encryptions and signatures in our work.

D. DATA REPLICATION MODULE

In this module, data replication becomes feasible through the enhanced precision of RSUs (Roadside Units) within the vehicle ad-hoc network, each equipped with its dedicated ad-hoc model for identifying and analyzing duplicate records. This process involves detecting matching records with other RSUs, thereby triggering the data replication module. Each RSU unit manages its specific vehicle ad-hoc network, and the Database Replication module is employed for importing data from pre-existing databases, even accommodating intricate mappings across multiple tables joins.

V. RESULT ANALYSIS

In order to determine the runtime of a loop, it is necessary to calculate the duration of the block of code contained within it and then multiply this value by the number of times the loop will be executed. Loops that exhibit a proportional growth in relation to the input size are characterized by a linear time complexity of O(n). Even if only half of an array is looped through, the time complexity remains O(n). Time complexity is a measure of the number of times a statement is executed within an algorithm. It is important to note that the time complexity of an algorithm does not reflect the actual time required to execute a specific code, as this is influenced by other factors. However, it can be stated with certainty that for any given input, the algorithm will return a result within a fixed and finite amount of time.

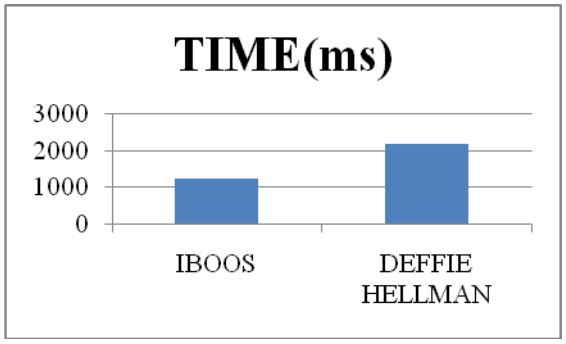
.

ALGORITHM	Time(ms)
IBOOS	1250
DEFFIE HELLMAN	2200

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302061 |



VI. FUTURE WORK

To devise and assess methodologies aimed at enhancing the scalability of the suggested approach. Potential strategies encompass the utilization of lightweight cryptography, optimization of the blockchain network architecture, or the development of a hybrid solution that amalgamates blockchain with other technologies, such as edge computing. Additionally, an investigation into the potential utilization of the proposed approach to support other applications within the Vehicular Ad-Hoc Network (VANET) domain, such as cooperative driving and traffic management, is warranted. For instance, the blockchain ledger could serve as a repository for storing and exchanging traffic data among vehicles and Roadside Units (RSUs), thereby contributing to the enhancement of traffic flow and safety.

VII. CONCLUSION

This paper introduces a novel blockchain-based area security trust model wherein a Querying vehicle initiates an area request to a nearby Roadside Unit (RSU). The RSU's responsibility is to assemble a group of cooperative vehicles to create anonymous secure areas, and the query results are subsequently relayed back to the querying vehicle. To enhance security and privacy, the system leverages certificates as aliases to prevent direct communication between vehicles, mitigating the risk of security breaches. Additionally, the utilization of anonymous cover areas provides protection against Location Service Providers (LSPs). The proposed system employs a thermal reactor consensus mechanism for blockchain maintenance, which, when compared to PoX, reduces resource consumption and enhances computational efficiency. Lastly, the paper introduces a trust management algorithm, validated through experiments.

REFERENCES

[1] Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in vanets, by S. R. Pokhrel and J. Choi, IEEE Trans. Commun., vol. 68, no. 8, pp. 4734-4746, Aug. 2020.
[2] M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud, and M. Abdallah, an energy-productive information sending technique for heterogeneous wbans," in Proc. IEEE Far off Commun. Netw. Conf. (WCNC), pages in April 2019, 1-7.
[3] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, tfppasv: a three-factor security safeguarding validation plot for vanet," Contraptions, vol. 9, no. 9, p. 1338, Aug. 2020
[4] X. Jiang, F. R. Yu, T. Tune, and V. C. M. Leung, bcppa: a blockchain-based restrictive protection safeguarding validation convention for vehicular impromptu organizations," IEEE Web Things J., early access, Sep. 24, 2020, doi: 10.1109/JIOT.2020.3026354.
[5] S. Ayvaz and S. C. Cetin, dad crt: chinese remaining portion hypothesis based contingent protection safeguarding verification plot in vehicular impromptu organizations," Int. J. Intell. Syst. automate, vol. 7, no. 2, pp. 72-87, Apr. 2019
[6] Zheng, D., Jing, C., Guo, R., Gao, S., & Wang, L. (2019). A traceable blockchain-based access authentication system with privacy preservation in VANETs. IEEE Access, 7, 117716-117726.
[7] Feng, Q., He, D., Zeadally, S., & Liang, K. (2020). BPAS: Blockchain assisted privacy-preserving authentication system for vehicular ad hoc networks. IEEE Transactions on Industrial Informatics, 16(6), 4146-4155.
[8] Cui, J., Zhang, X., Zhong, H., Zhang, J., & Liu, L. (2020). Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 2, February 2024 ||

| DOI:10.15680/IJIRSET.2024.1302061 |

[9] Dai, H., Zheng, Z., & Zhang, Y. (2019). Blockchain for internet of things: A survey. IEEE Internet of Things Journal, 6(5), 8076-8094.
[10] Xu, Z., Liang, W., Li, K., Xu, J., & Jin, H. (2021). A blockchain-based roadside unit-assisted authentication and key agreement protocol for Internet of vehicles. Journal of Parallel and Distributed Computing, 149, 29-39.
[11] In their article titled "DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain," C. Lin, D. He, X. Huang, M. K. Khan, and K. R. Choo discuss the development of a payment system that ensures both security and efficiency.
[12] The article "Smart contract development: Challenges and opportunities" by W. Zou, D. Lo, P. S. Kochhar, X. D. Le, X. Xia, Y. Feng, Z. Chen, and B. Xu explores the difficulties and potential benefits of smart contract development..
[13] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke delve into the research issues and challenges surrounding blockchain advancements for the web of things in their article titled "Blockchain advances for the web of things: Research issues and difficulties."
[14] T. H. Vo, W. Fuhrmann, and K.- P. Fischer-Hellmann present their work on privacy-preserving client character in Identity-as-a-Service in their paper titled "Privacy-preserving client character in Identity-as-a-Service."
[15] X. Zhu and Y. Badr conduct a study on titled "Character management systems for the Internet of Things: A study towards blockchain arrangements." The article was published in Sensors in 2018

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details