SMART CONTRACT-BASED FREE PRIVILEGE-PASS AUTHENTICATION SYSTEM FOR INDIAN RAILWAY USING PERMISSIONED BLOCKCHAIN

Hemraj Shobharam Lamkuche[1], Suneel Prasad
Symbiosis Centre for Information Technology Pune

ABSTRACT
Indian Railways conducts one of the world's largest recruitment drives annually across several railway zones. Each railway employee gets free and discounted travel everywhere in India. The corresponding railway zone issues free Privilege Pass/PTO certificates. Each employee benefits. E-Pass Verification ensures the authenticity of a railway authority's certificate. E-Pass verification affects deal authenticity. Illegals can benefit from discarded data. We proposed implementing and issuing E-Passes to railway employees using Blockchain Technology to solve this problem of forged E-Passes. It is one of the latest technologies that provide provenance and tamper-proof security. To verify that data's fidelity, we use a blockchain hash affirmative method. The blockchain's prominence aids in the abolition of bogus E-passes. In this research article, the author used a permissioned public blockchain platform known as Hyper-Ledger for E-Pass authentication and verification. The system is more secure, and only legitimate railway employees verified by the CRIS (Centre for Railway Information Systems) system can join the network. The authenticity of information can be ensured by verifying distributed ledger technology against the hash in the blockchain at any moment.

KEYWORDS: Permissioned Blockchain, Smart Contract, Indian Railway, Reservation System, Hyperledger Fabric

MSC: 62-P25

RESUMEN
Indian Railways lleva a cabo anualmente una de las campañas de reclutamiento más grandes del mundo en varias zonas ferroviarias. Cada empleado ferroviario obtiene viajes gratis y con descuento en todas partes de la India. La zona ferroviaria correspondiente emite certificados Privilege Pass/PTO gratuitos. Cada empleado se beneficia. E-Pass Verification garantiza la autenticidad del certificado de una autoridad ferroviaria. La verificación de E-Pass afecta la autenticidad del trato. Los ilegales pueden beneficiarse de los datos desechados. Propusimos implementar y emitir E-Passes a los empleados ferroviarios utilizando la tecnología Blockchain para resolver este problema de E-Passes falsificados. Es una de las últimas tecnologías que proporciona seguridad de origen y a prueba de manipulaciones. Para verificar la fidelidad de los datos, utilizamos un método afirmativo de hash de blockchain. La prominencia de la cadena de bloques ayuda a abolir los pases electrónicos falsos. En este artículo de investigación, el autor utilizó una plataforma de cadena de bloques pública autorizada conocida como Hyper-Ledger para la autenticación y verificación de E-Pass. El sistema es más seguro y solo los empleados ferroviarios legítimos verificados por el sistema CRIS (Centro de Sistemas de Información Ferroviaria) pueden unirse a la red. La autenticidad de la información se puede garantizar mediante la verificación de la tecnología de registros distribuidos contra el hash en la cadena de bloques en cualquier momento..

PALABRAS CLAVE: Cadena de bloques autorizada, contrato inteligente, ferrocarril indio, sistema de reservas, Hyperledger Fabric.

1. INTRODUCTION

In recent years, IT has aided in the digitization of technology. Data security is more crucial than ever before. People's lives have been made more accessible and more comfortable by advances in information technology, internet connectivity, computers, and mobile gadgets [1]. Virtual currency, originally developed for online use as a digital coin, has introduced a new dimension to innovation. It uses the most popular blockchain technology [2]. Blockchain's decentralized, distributed, the integrated database has many uses. This technology records transactions. Once the nodes agree, it becomes a dependable and secure block. A blockchain has numerous blocks, each with two sides. The next block's heading hashes the first block's data. so that all the blocks form a blockchain. Each block's data is decentralized across nodes so they may maintain a database. Once a block is validated by more than one block, it becomes valid and cannot be modified. A blockchain-based rail pass system, for example. It dispels doubts regarding information's validity. We must retain reputation, faith in certification, and proof of learning as education becomes more diverse, decentralized, and democratized. Every Indian railway employee needs a free permit to ride free. Authenticity, trust, accessibility, and security are issues. A digital signatures, secure databases, blockchain technology, and permissioned blockchain are countermeasures. [3].
There is a great need of privilege pass for travelling to various destination in the country, different state, and union territory, and now a days due to digitalization, the hardcopies of privilege pass are often seen [4].

[1] hemraj.lamkuche@gmail.com | suneel@scit.edu

If your card is lost or destroyed, you must apply in person. Re-application becomes significantly more complex and time consuming in this circumstance. This is due to the fact that certificates are issued by numerous organizations and concern railway authorities. In contrast, applying for an online privilege pass is much more time-consuming, paper-saving and easier through HRMS system (Human Resource Management System) of Indian Railway which is managed by Centre for Railway Information Systems (CRIS) [5]. This is because any privilege pass can be easily applied for by providing the information required for identity verification. However, for this facility, fake testimonials and fake privilege pass are in vogue.

This research paper aims to understand the blockchain and Ethereum in building the smart contracts. The above introduction provided the primary purpose and reason behind the study. The paper has been subdivided into several sections which covers objectives of the study ranges from: Checking the validity of the issuing authority of privilege pass, to detect the issuing authority are not fake or illegitimate, Railway employee capability to control issuing of privilege pass through online portal which is manages by HRMS system, and also to ensure data transparency, data security and privacy should be maintain throughout using blockchain distributed ledger.

2. INDIAN RAILWAY PRIVILEGE PASS SYSTEM

Indian railway employees get free privilege passes. A Ministry of Railways Privilege Pass permits free rail travel. A privilege ticket can be redeemed for a passenger rail ticket at one-third the standard rate. A railway servant is a member of a service or someone who works for the Railway Board. This term excludes anyone loaned from a service or post not under Railway Board administrative authority to one that is. [6]. Special-ordered casual labour isn't included. A recognized educational institution is any school, college, university, or other government-recognized institution that provides general, technical, professional, or military education or training. Any officer or authority designated by the Central Government (Ministry of Railways) may grant or sign a pass or PTO (Ministry of Railways). Until such authorities or officers are found, the Pass or PTO shall be signed and granted in accordance with the Ministry of Railways' instructions/orders in effect when these Rules were adopted. [6]. The following types of passes may be provided to a railway servant or the eligible members of his or her family and dependent relations as described in these Rules: Duty pass, Privilege pass including passes while on deputation, School pass, Post-retirement Complimentary pass, Widow pass, Residential card pass, and Special pass.

3. LITERATURE REVIEW

3.1. Research Review

The blockchain certificate system proposed in this article is a set of certificate systems based on blockchain, as opposed to current traditional certificate systems and other blockchain alternatives [7]. Technology that fully embraces the smart contract and is independent of any other third-party system, can fit the needs of real-world applications, and overcomes the problems with the existing traditional electronic certificate system in the blockchain certificate system advances blockchain technology's practical application in education, where there is much guidance. It's important. Current system focuses primarily on certifications; future system will be broader. Smart contracts can be used to define roles and delegate authority management, data protection, and anti-tampering. IoT components include: Devices have security flaws, but blockchain-based authority management could fix problems and protect privacy. [7],[8],[3].

Utilizing the uprightness cross section of the exchanges, an entire setup of worth exchanging advancements are starting to enter the market. The vital development here is Smart Contracts [9],[10]. Blockchain's ability to monitor product information in supply chain management has the potential to alter how information is transmitted among chain participants. [11]. The world is slowly but surely transforming. Cryptocurrencies are affecting the economy in a big way [12]. The authors study educational institutions where students use government-approved IDs. College authorities physically evaluate previous degree certificates during admissions. This is time-consuming. [13]. In our suggested research, we focused on implementing a permissioned blockchain platform in the light of hyper-ledger to issue and validate digital free privilege passes to railway employees. In the suggested system, unauthorized parties cannot access data. Only trusted participants can access Free Privilege Pass data.

3.2. Blockchain Technology

In 2008, under the name of Satoshi Nakamoto an author posted online an article titled, ”A Peer-to-Peer Electronic Cash System,” the writer discusses a digital currency known as Bitcoin which is transferred among people via a trusted networks [1]. The Blockchain enables members to keep a database of goods based on consensus. This consensus derives from the necessity for majority participation in database extensions. No minority may compromise the database's data, make illegal changes, or discontinue its

maintenance. Bitcoin, Ethereum, Dogecoin, Litecoin, and others use Blockchain. Every transaction in this record is authorized by the owner's electronic signature, which confirms and protects it. [2], [12]. The computerized record's data is safe. Multiple exchanges' information is stored in squares alongside its date; each transaction can be separately confirmed by using its hash esteem. Since it's open, freely irrefutable, and the information once input cannot be amended, it helps prevent fraud. In blockchain, each block of transactions is linked by its hash value as shown in figure 1.

3.3. Ethereum

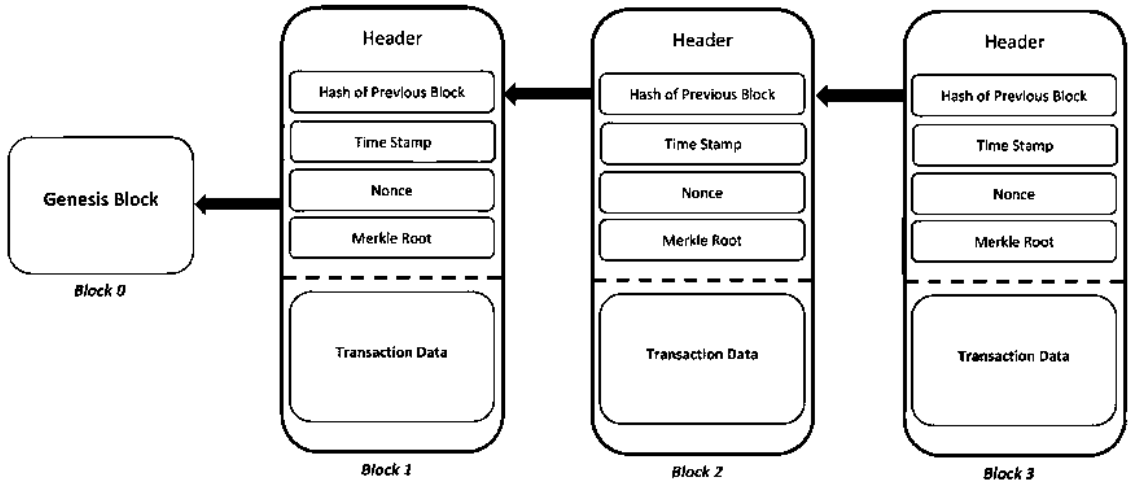

Figure 1: Anatomy of Block in Blockchain

In 2013, Vitalik Buterin and others invented Ethereum [2]. Everyone on the Ethereum network has an identical copy of the ledger, allowing them to view all transactions. Decentralized means that all distributed ledger owners run and maintain the network. Cryptography secures and verifies blockchain transactions. Computers mine, or solve complicated mathematical equations, to confirm network transactions and add new blocks to the blockchain. Participants are awarded cryptocurrency tokens. Ethereum tokens are called Ether (ETH). Ether can be used to buy and sell like Bitcoin. Its rising price makes it a speculative investment. Ethereum users can construct apps that "run" on the blockchain like computer software. These program store and transport personal data and conduct financial transactions. Ethereum permits network computations during mining, unlike Bitcoin. This transforms a value store and medium of exchange into a decentralized global computing engine and freely verifiable data storage. [2], [7], [9].

3.4. Smart Contracts

A smart contract is a computer program having self-verifying, self-executing, tamperproof properties. The smart contract concept was proposed by Nick Szabo [14]. A smart contract is a software program that is run on top of the Blockchain [15]. It contains a set of rules which are agreed upon by the involved parties (miners), specifying how they should interact with each other and the chain on certain conditions. The code will be executed by miners when a particular event occurs. It takes transaction as an input, executes the corresponding code and triggers the output events. Depending upon the function logic implementation states are changes. The programming language Solidity is used to implement the smart contract in various blockchain platforms [7][15].

4. BLOCKCHAIN BASED PRIVILEGE PASS SYSTEM

This section introduces the study methodology for this research. There are two methods by which we chose to achieve the study goals, that are system design and verification process. The major objective of this research is to use permissioned blockchain platform to issue, manage, and verify free privilege pass issued by Indian Railway to Railway Employee. Moreover, it presents the overall workflow of the architecture.

4.1. Architectural Design

We propose a unique architecture that improves and enhances the trust and openness of traditional privilege pass management systems in Indian Railway and Concern offices of various zones. The proposed architecture embedded with several methods like input, write, validate and confirm in a Quad-phase style. These approaches are defined below as.

Input: It is the same in both architectures, where privilege pass official data, such as Journey, employee

identification, and privilege pass information, are input from a desktop application or web-based system. Note that Indian railway institutions control those input applications. The possible actors of such applications are Privilege Pass authority office, divisional managers or issuing authority, and clerks.

***Write*:** In the conventional approach, input data is written by privilege pass issuing clerk manually on an authorized paper which is again counter-signed by Issuing authority and sealed using stamp. The privilege pass validity is limited to 4 months from the issued date. Now due to online approach, the clerical staff uses desktop application or mobile based application to issue free privilege pass using HRMS system. In our approach, however, data is written to both the local database and blockchain. The input data is converted through our data mapping structure.

***Validate*:** After the input data is matched with the data structure of HRMS system, its format and signature are checked. That input data becomes a transaction in our blockchain. Note that the electronic signatures are provided and ensured by Indian Railway centralized authentication system (i.e., HRMS System). By identifying the employee details using employee ID, PAN number, Aadhar number, Date of birth, Date of Joining and other related information stored on HRMS system. The data stored on the blockchain is trustworthy and tamperproof.

Confirm: Validated transactions are put into a block, and a new block is created to confirm those transactions which were requested for issuing free privilege pass on the account of each railway employee. After confirming the above process, the data which stores on blockchain become permanent and it became impossible to change the data, and any modification on the existing data on respective block is recorded on the distributed ledger.

The decentralized application was programmed on the Ethereum platform and is executed by

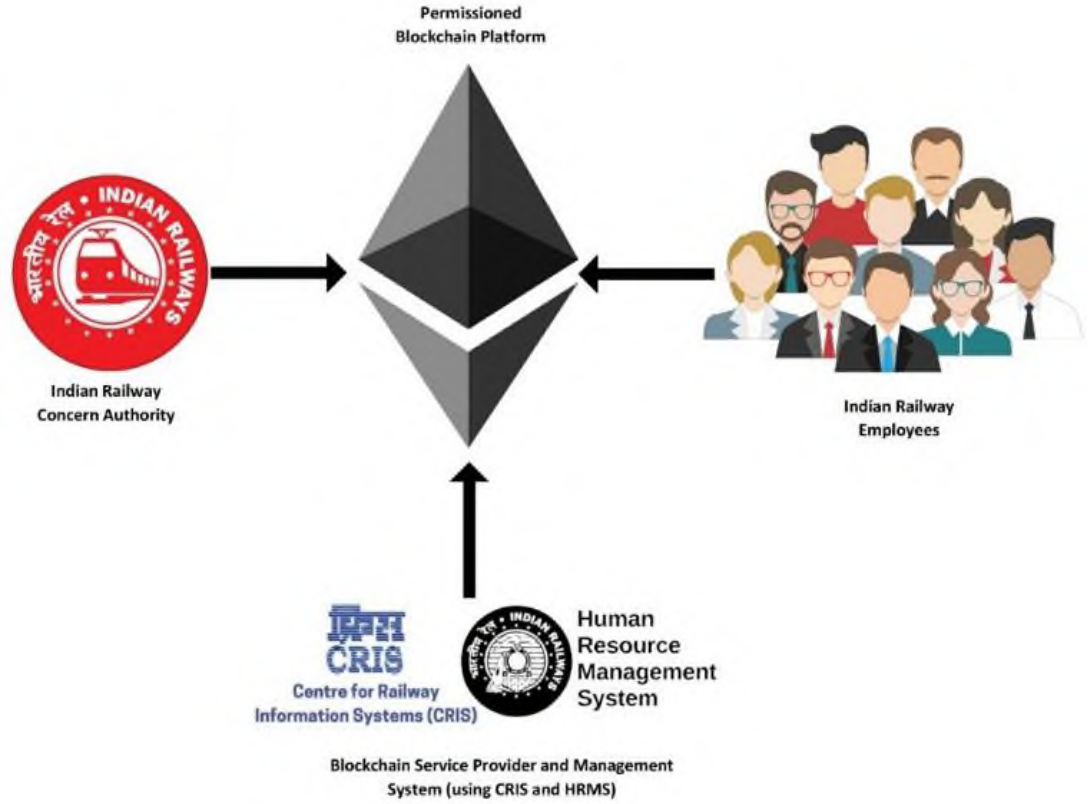

Figure 2: Permissioned Blockchain based free privilege pass system

using Ethereum virtual machine (EVM), where the smart contract is executed whenever condition satisfies [16]. In the proposed system, multiple entity is involved, Issuing Authority who have access to the system, they can also retrieve the decentralized database. When Indian railway employee fulfilled certain requirements for issuing free privilege pass, the concern authorities grant a free privilege pass through the blockchain based decentralized system. Once the free privilege pass is issued and received by the employee, the concern employee can itself track and check the validity of the requested privilege pass via same decentralized application. Similarly, the concern railway authority can also do the verification process of the issued privilege pass using same portal through mobile or web-based decentralized application.

The blockchain validates and confirms the transactions in the network with its peers, complete nodes, and certificate authority are blockchain components. The said decentralized software can

be implemented on Hyperledger Fabric, Quorum, Ripple, and other permissioned blockchains. Free privilege pass authentication is a railway zone and divisional railway management procedure; thus, it requires high-level examination and verification, which HRMS can handle simply. In our suggested system, we recommend employing open-source platforms like Ethereum as indicated in figure 2 above.

4.2. Privilege Pass Verification System

Indian Railway's present infrastructure is well-suited for permissioned blockchain networks since free

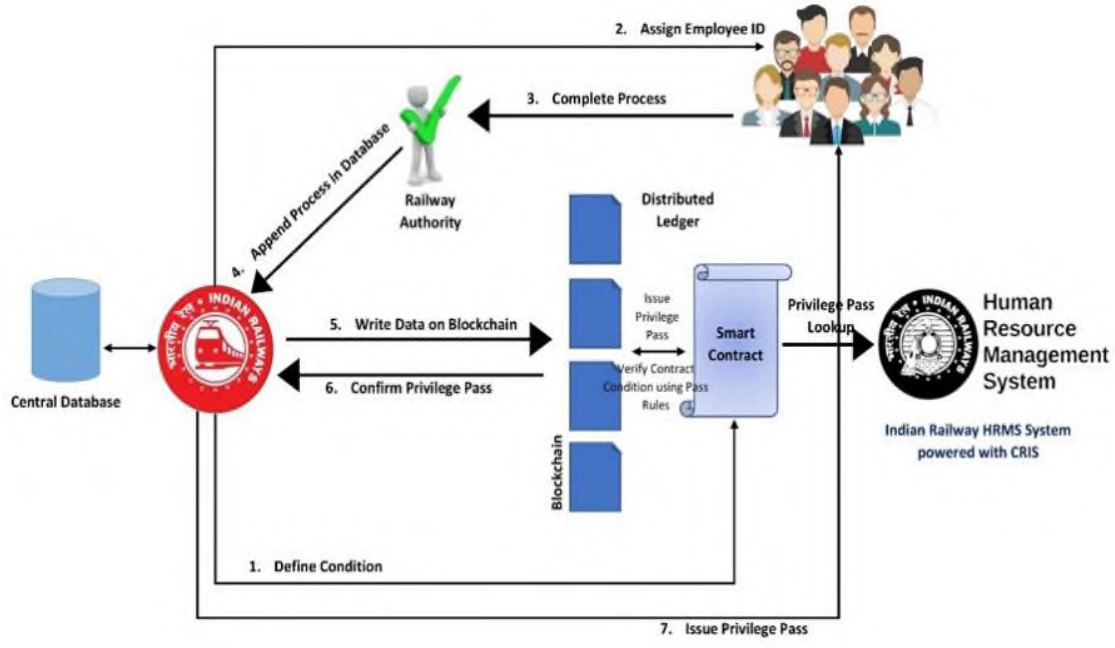

Figure 3: Verification process in blockchain-based free privilege pass system

privilege passes must be checked by HRMS. Because free privilege passes aren't issued in real-time, network and transaction performance can be intermediate. Since the aforementioned system uses a permissioned blockchain network, the consensus mechanism might be proof of stake. Employees and authorities must register to join the private network. The Indian Railway HRMS system offers an admin position to assign blockchain read/write permissions. The HRMS decision must be validated by the issuer. The HRMS system checks if the issuing clerk or officer's signature is validated and if the same individual can issue a free privilege pass to a railway employee. Figure 3 describes the overall system for verification and issuing of free privilege pass to railway employee.

There are several entities involve in the proposed system, including Indian Railway, Railway Employees, Clerks and Concern Authority, Issuing Authority, and Privilege Pass verification entity. The HRMS system play the role of defining training smart contract conditions, which point out the number of free privileges passes or Privilege ticket order can be issued on the account for railway employee for the financial year. In other words, this contract defines privilege pass issuing programs with a set of variables. The employee must complete the contract conditions through online system which is again managed by HRMS system. When an employee enrolls in serving railway as a full-time employee, then according to the rules laid down under free privilege pass rules, it is mandatory for administration to issue free privilege pass to railway employee as per their request. As a concrete system design, each zone of railway has a local database that provides a data repository for its human resource management system i.e., HRMS system which is again connected to centralized HRMS system. Thus, all the related information of an employee is stored on the block in blockchain by using details like employee ID, department name, timestamp (at the time of registering employee data in HRMS system). These values will be hashed together to create the identification key of the employee in the blockchain network. In our proposed operation process system, the employee will do several assessments assigned by concern higher privilege pass issuing authority. Once the employee clears the verification process, the concern authority will write the entry of privilege pass into a local database of the HRMS system. Through the data model presented hereafter, the HRMS system data will automatically be transferred to our proposed system.

Once all employee record smart contract conditions are completed, a privilege pass transaction is automatically created and stored on the blockchain. Our data mapping structure from Indian railway staff management system to blockchain data will send privilege pass issue information to zonal and divisional railways. Using blockchain technology, privilege pass information is distributed and confirmed by blocks

on decentralized peer nodes. The data written on the block cannot be modified by third parties or intruders. Based on the privilege pass information on the blockchain network, the HRMS system will deliver both a digital document with a QR code and an SMS to the employee's registered phone. HRMS systems can query blockchain transactions using employee privilege pass codes to check issued privilege passes. The suggested method uses asymmetric encryption to safeguard digital privilege passes. [17]–[19]. The HRMS system also uses its key (i.e., electronic signatures provided by Indian Railway system) combining with the concern authority keys to write data in the blockchain system. This mechanism helps prevent fake transactions during writing data of concern privilege pass issuing authority on the local railway system database and from the local database to the blockchain network.

4.3. Data Privacy in Privilege Pass System

In our suggested solution, HRMS system owners can grant access to other employees. To do this, we use Permission asset, which sets employee access levels for blockchain-stored free privilege passes. Our suggested system generates a permission asset for each privilege pass transaction. A permission asset stores three important information, covering (i) ID of employee, (ii) ID of Issuing Authority, which determines the owner of the corresponding zone or divisional railway office and, (iii) a list of employees who can read the data from the blockchain network. The HRMS system can manage this list by removing a user or adding a new user.

5. EXPERIMENTAL RESULTS

We execute our research on a Hyperledger Fabric cluster in this approach of evaluations and tests. To host our cluster system, we employ three cloud computing instances created with Amazon Web Services instances on Amazon EC2. Each instance has 16 virtual CPUs and 32 GB of RAM [20]. As a result, we use docker to start Hyperledger fabric. Measurement of TCP performance, publishing transactions onto distributed ledger and reading grade and degree from the ledger, and the impact of resource allocation on performance can all be done with the help of Hyperledger fabric [21]. For each experiment, we track throughput and latency. To achieve the required results, each parameter setting was run numerous times. The goal of this experiment is to demonstrate that the cluster's network performance is quick, and that node communication delay is modest enough to be excluded from the total latency measured in the Hyperledger Fabric-based blockchain network. On Amazon EC2, we set up two fresh Ubuntu instances for our testbed. Other than our experiment, there is no other traffic. The network is fast among Amazon EC2 nodes, with a peak speed of up to 8,000 Mbps. To determine throughput, we increase message size in each configuration (in order to provide extensive information about an employee for the purpose of issuing a free permission pass) and calculate throughput [22]–[25]. Because the transaction size of Hyperledger Fabric is only 3 KB, we set the message size to 3 KB for latency. When the message size exceeds the MTU (1,500 bytes) for ethernet, the speed decreases significantly to 1,000 Mbps. This is why we chose a message size of 3 KB, which allows us to strike a balance between throughput and delay. The goal is to demonstrate whether or not scalability can be achieved by allocating more resources to each peer node. For each configuration, we set the transaction rate and adjust the number of virtual CPUs and RAM. Virtual CPUs range from one to sixteen cores, with RAM sizes ranging from one to 32 gigabytes. When we change the setup, we can boost throughput and lower latency [26], [27].

6. CONCLUSION

In this paper, we describe the free privilege pass and fake pass authentication problems on the Indian Railways. We proposed our prototype system called the Free Privilege Pass System, based on a permissioned blockchain application dealing with the problem of the fake privilege pass mentioned above. Although the proposed system was developed to suit Indian railway conditions, the principal designs can also be inherited in privilege pass authentication systems in other departments of the Indian Railway for verifying privilege features provided to employees during their service tenure. The proposed system is more reliable, transparent, and immutable as it will not require any third-party intervention. The proposed system also acts as a paper-saving model that will verify a person's true identity through a QR code or serial number and provide a privilege pass that is time-saving. It will be hassle-free and will be better than the previous digital system provided by the CRIS and HRMS systems of Indian Railways.

RECEIVED: DECEMBER, 2021.
REVISED: MARCH, 2023.

REFERENCES

[1] BUTERIN, V. (2014): A next-generation smart contract and decentralized application platform, **Etherum**, no. January, 1–36.

[2] BASUMATARY S, P. S. (2019): Performance evaluation and benchmarking of hyperledger fabric - **Master's thesis, Indian Institute of Technology Hyderabad, India**.
[3] CANRIGHT, D. (2005): A Very Compact S-Box for AES," **Cryptogr. Hardw. Embed. Syst. – CHES 2005**, 3659, 441–455s.
[4] CHEN, G., XU, B., LU, M. and CHEN, N. S. (2018):Exploring blockchain technology and its potential applications for education, **Smart Learn. Environ.**, 5(1), 1–10.
[5] CHRISTIDIS, K. and DEVETSIKIOTIS, M. (2016): Blockchains and Smart Contracts for the Internet of Things, **IEEE Access**, 4, 2292–2303.
[6] DEENMAHOMED, H. A. M., DIDIER, M. M. and SUNGKUR, R. K. (2021): The future of university education: Examination, transcript, and certificate system using blockchain, **Comput. Appl. Eng. Educ**., 29(5), 1234–1256.
[7] DALAL, J., CHATURVEDI, M., GANDRE, H. and THOMBARE, S. (2020): Verification of Identity and Educational Certificates of Students Using Biometric and Blockchain, **SSRN Electron. J**.
[8] EA, B. (015): Kubernetes and the path to cloud native, **Proc. sixth ACM Symp. cloud Comput**., 167.
[9] . HUANG B, K. M. and BAUER, M. (2005): Hpcbench-a Linux-based network benchmark for high performance networks, 19th **Int. Symp. high Perform. Comput. Syst. Appl. - IEEE**, 65–71.
[10] KEHRLI, J. (2016): Blockchain 2.0-From Bitcoin Transactions to Smart Contract applications.
[11] KUZLU M, R. S., PIPATTANASOMPORN, M., GURSES, L. (2019): Performance analysis of a hyperledger fabric blockchain framework: throughput, latency and scalability, **IEEE Int. Conf. blockchain (Blockchain). Piscataw**., 536–540.
[12] KOSBA, A., MILLER, A., SHI, E., WEN, Z. and PAPAMANTHOU, C. (2016): Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts, **Proc. - 2016 IEEE Symp. Secur. Privacy, SP**, 839–858.
[13] KUMAR, S., KUMAR, D. and LAMKUCHE, H. S. (2021): TPA Auditing to Enhance the Privacy and Security in Cloud Systems, **J. Cyber Secur. Mobil**., 10(3).
[14] LAMKUCHE, H. S. and PRAMOD, D. (2020): Csl: Fpga implementation of lightweight block cipher for power-constrained devices, **Int. J. Inf. Comput. Secur.,** 12(2–3).
[15] LAMKUCHE, H. S., PRAMOD, D., ONKER, V., KATIYA, S. A., LAMKUCHE, G. S., and HIREMATH, G. R. (2019): SAL – A lightweight symmetric cipher for Internet-of-Things," **Int. J. Innov. Technol. Explor. Eng.**, 8(11) Special Issue.
[16] LAMKUCHE, H. S., KONDAVEETY, V. B., SAPPARAM, V. L., SINGH, S. and RAJPURKAR, R. D. (2022): Enhancing the security and performance of cloud for e-governance infrastructure: Secure E-MODI, **Int. J. Cloud Appl. Comput.,** 12(1).
[17] MOHANTA, B. K. and JENA, D.(1018): An Overview of Smart Contract and Use Cases in Blockchain Technology, 2018 **9th Int. Conf. Comput. Commun. Netw. Technol.,** 1–4.
[18] NAKAMOTO, S. (2008): Bitcoin: A Peer-to-Peer Electronic Cash System, **Artif. Life**, 1–9.
[19] POPOV, S. (2018): IOTA Whitepaper v1.4.3, **New Yorker**, 81(8), 1–28.
[20] POSCHMANN, A. (2009): Lightweight Cryptography: Cryptographic Engineering for a Pervasive World, **Ruhr-University Bochum**.
[21] RAILWAY, I. (1986): RAILWAY SERVANTS (PASS) RULES,1986 (1993 EDITION).
[22] RAILWAY, I. (2020): What is HRMS? Human Resource Management System of Indian Railway, **Indian Railway - Railway Ministry**.
[23] REIS-MARQUES, C. and FIGUEIREDO, R. (2021): Applications of Blockchain Technology to Higher Education Arena : A Bibliometric Analysis, **Eur. J. Investig. Heal. Psychol. Educ.,** 11(4), 1406–1421.
[24] RIVEST, L. A., RONALD, L., and SHAMIR, A. (1978): A method for obtaining digital signatures and public-key cryptosystems., **Commun. ACM**, 21(2), 120–126.
[25] SARMA, S. N. S., LAMKUCHE, H. H. and UMAMAHESWARI, S. (2013): A review of secret sharing schemes," **Res. J. Inf. Technol.**, 5(2).
[26] SZABO, N. (1997): Formalizing and securing relationships on public networks," **First Monday**.
[27] XIE, R. ET AL. (2020): Ethereum-Blockchain-Based Technology of Decentralized Smart Contract Certificate System, **IEEE Internet Things Mag**., 3(2), 44–50.