A NOVEL METHOD FOR VERIFYING CERTIFICATES USING BLOCK CHAIN

V. Padmaja, Assistant Professor, Department of Computer Science and Engineering DVR & Dr. HS MIC College of Technology, Kanchikacherla, Andhra Pradesh, India
Dr.G.Sai Chaitanya Kumar, Associate Professor, Department of Computer Science and Engineering, DVR & Dr. HS MIC College of Technology, Kanchikacherla, Andhra Pradesh, India
Shaik sama,Y prathyusha,B. Mohan, V. Vasu, UG Students, Department of Computer Science and Engineering DVR & Dr. HS MIC College of Technology, Kanchikacherla, Andhra Pradesh, India.

Abstract:
In this project to secure academic certificate and for accurate management and to avoid forge certificate we are converting all certificates into digital signatures and these digital signatures will be stored in Blockchain server as this Blockchain server support tamper proof data storage and nobody can hack or alter its data and if by a chance if its data alter then verification get failed at next block storage and user may get intimation about data alter.
In Blockchain technology same transaction data stored at multiple servers with hash code verification and if data alter at one server, then it will be detected from other server as for same data hash code will get different. For example, in Blockchain technology data will be stored at multiple servers and if malicious users alter data at one server, then its hash code will get changed in one server and other servers left unchanged and this changed hash code will be detected at verification time and future malicious user changes can be prevented.
In Blockchain each data will be stored by verifying old hash codes and if old hash codes remain unchanged then data will be considering as original and unchanged and then new transaction data will be appended to Blockchain as new block. For each new data storage all blocks hash code will be verified.

1.Introduction:

Counterfeit academic certificates have been a longstanding issue in the academic community. Not until the Massachusetts Institute of Technology Media Lab released their project of Block-certs, a technique which is mainly implemented by conflating the hash value of local files to the blockchain but remains numerous issues, did an effective technological approach protecting authentic credential certification and reputation appear. Based on blockcerts a series of cryptographic solutions are proposed to resolve the issues above, including, utilizing a multi-signature scheme to ameliorate the authentication of
certificates; exerting a safe revocation mechanism to improve the reliability of certificates revocation; establishing a secure federated identification to confirm the identity of the issuing institution.

1.1 Overview:

The project consists in designing and implementing the system which covered the above solutions. The project also involves a comprehensive evaluation of the system security, and the assessment outcomes provide compelling evidence to prove that implementation is practical, reliable, secured, which might give some hints of important architectural considerations about the security attributes of other blockchain-based systems.In this section, we discuss the implementation from the point of view of system architecture, database architecture. The system architecture and database architecture show how the system is designed from the engineering point of view.The issuing applications are responsible for the main business logic which include the certificates applying, examining, signing and issuing. The issuing applications are designed to merge the hash of the certificate in a Merkle tree and send the Merkle root to Blockchain amidst signing by the majority of community members. Also, the issuing applications involved the revocation of certificate. The issuing applications are responsible for the main business logic which includes the applying for, examining, signing and

 DOI: 10.36893.DRSR.2023.V13I04.0036-0039

issuing of the certificates. The issuing applications are designed to merge the hash of the certificate with a Merkle tree and send the Merkle root to the Blockchain. Also, the issuing applications deal with the revocations of certificates.

Methodology:

1) Save Certificate with Digital Signature:
   Using this module admin user can upload student details and student academic certificate and then application convert certificate into digital signature and then signature and other student details will be saved in Blockchain database.
2) Verify Certificate: In this module verifier or companies or admin will take certificate from student and then upload to application and then application will convert certificate into digital signature and this digital signature will get checked/verified at Blockchain database and if matched found then Blockchain will retrieve all student details and display to verifier and if match not found then this certificate will be consider as fake or forge.

Modules Used in Project: -

1. Tensorflow
2. Numpy
3. Pandas
4. Matplotlib
5. Scikit learn

2.Related work:

In health field, medical history of each patient must be treated with utmost confidentiality. Blockchain technology is used as a distributed approach to provide security for the medical reports of patients. Security is implemented in a three phased manner which includes authentication, encryption[8] and data retrieval. Quantum cryptography and Advanced Encryption Standard (AES) encryption are used for ensuring a secure transaction for end users. Data retrieval is realized using SHA algorithm [1]. Financial institutions have also started adopting blockchain technology to avoid issues of network attackers and security-based issues faced in online transactions. Digital currency called bitcoin ensures a peer to peer distributed and decentralised of payment scheme. Such a network offers added advantages of immutability, reduced charges imposed by third parties and faster transactions. Confirmation of an electronic payment is based on cryptographic proof and no third party is involved which offers a reliable payment platform. Issue of double spending is also avoided by means of distributed timestamp server which generated the computational proof of transaction in chronological order. Users can validate their identity by means of digital signature. Private key will be used by each user to perform a transaction while other nodes will check for the authenticity of the payment by checking the public key of the user. If an attacker wants to interfere with a transaction block, POW of all previous blocks and all blocks after it must be redone along with suppressing the work of honest nodes. This cannot be done without the consensus of entire network and hence attacking a blockchain network becomes a tedious task [2].

3.Proposed model:

In this model, a blockchain certificate system was developed based on relevant technology. The system's application was programmed on the Ethereum platform and is run by the EVM. In the system, three groups of users are involved, Schools or certification units grant certificates, have access to the system, and can browse the system database. When students fulfilled certain requirements, the authorities grant a certificate through the system. After the students have received their certificate, they are able to inquire about any certificate they have gained.

3.1Algorithm used:

SHA512: we use sha512 algorithm for generating hashvalue.it is a hashing algorithm that performs a hashing function on some data given to it. Hashing algorithms are used in many things such as digital certificates. hashing algorithms plays a vital role in digital security.

 DOI: 10.36893.DRSR.2023.V13I04.0036-0039

1. SHA 512 works in 4 stages
- Input formatting
- Hash buffer initialization
- Message processing
- Output

Input formatting: SHA-512 can't actually hash a message input of any size, i.e., it has an input size limit. This limit is imposed by its very structure as you may see further on. The entire formatted message has basically three parts: the original message, padding bits[6], size of original message. And this should all have a combined size of a whole multiple of 1024 bits. This is because the formatted message will be processed as blocks of 1024 bits each, so each bock should have 1024 bits to work.
Hash buffer initialization: The algorithm works in a way where it processes each block of 1024 bits from the message using the result from the previous block. Now, this poses a problem for the first 1024-bit block which can't use the result from any previous processing. This problem can be solved by using a default value to be used for the first block in order to start off the process.
Message processing: Message processing is done upon the formatted input by taking one block of 1024 bits at a time. The actual processing takes place by using two things: The 1024-bit block, and the result from the previous processing[5]. This part of the SHA-512 algorithm consists of several 'Rounds' and an addition operation.
Output: After every block of 1024 bits goes through the message processing phase, i.e., the last iteration of the phase, we get the final 512-bit Hash value of our original message. So, the intermediate results are all used from each block for processing the next block[7]. And when the final 1024-bit block has finished being processed, we have with us the final result of the SHA-512 algorithm for our original message.

4.Results and discussion:

Our application has three pages: an admin login page, an add student and certificate page, and a final verifier page. With the admin login id and password, the admin can access our programme. The administrator can then tap the add student and add certificate button to add the students and their certificates.The verifier can then use the verifier login information and password to validate the certificate. They enter the student's login ID, choose the type of certificate, and then hit the "verify" button.
The outcome will be successful if the certificates that were uploaded are authentic. If not, the outcome will be adjusted and incorrect

5.Conclusion:

We infer from the above data that XGB Classifier and Logistic Regression produced the same outcomes. As a result of its excellent accuracy and efficiency, the XGB Classifier is a potent machine learning algorithm for classification tasks that has grown in popularity in recent years. When using XGB Classifier, there are a number of critical procedures that must be taken, including as gathering and preprocessing data, choosing pertinent features, and fine-tuning the model's hyperparameters for optimum performance. Due to its integrated regularisation approaches XGB Classifier has the capacity to accommodate missing data and prevent overfitting, which is one of its main advantages. XGB Classifier is a suitable option for big data applications because it can also handle enormous datasets with high dimensions.
However, mastery in machine learning and data analysis is also necessary for using XGB Classifier, as well as knowledge of the specific domain and the dataset being used. It is important to carefully select the right features and hyperparameters to avoid underfitting or overfitting the model.
Overall, XGBClassifier is a valuable tool for building accurate and efficient classification models, and its popularity is likely to continue to grow as more applications are found for this powerful algorithm.Our work has really become easy by using google Collaboratory because it is an open-

DOI: 10.36893.DRSR.2023.V13I04.0036-0039

source library and installation of libraries will be very easy and cell by cell execution was done which helps us to find errors easily in each part of our code have a look at our work: https://colab.research.google.com/drive/19SAREEGPMAMAxax1lP61wyPMfPiZOhwq?usp=sharing

References:

[1] Jiin-Chiou Cheng; Narn-Yih Lee; Chien Chi; Yi-Hua Chen, "Blockchain and Smart Contract for Digital Certificate" IEEE International Conference on Applied System Invention (ICASI),2018.

[2] Wang Z., Lin J., Cai Q., Wang Q., Jing J., Zha D. (2019) Blockchain-Based Certificate Transparency and Revocation Transparency. In: Zohar A. et al. (eds) Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science, vol 10958. Springer, Berlin, Heidelberg.

[3] D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay, "Certificate Transparency Using Blockchain," 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, Singapore, 2018, pp. 71-80, doi: 10.1109/ICDMW.2018.00018.

[4] Aisong Zhang and Xinxin Ma, "Decentralized Digital Certificate Revocation System Based on Blockchain", Journal of Physics: Conference Series, Volume 1069, 3rd Annual International Conference on Information System and Artificial Intelligence (ISAI2018) 22–24 June 2018, Suzhou.

[5] G.Sai Chaitanya Kumar, Dr.Reddi Kiran Kumar, Dr.G.Apparao Naidu, "Noise Removal in Microarray Images using Variational Mode Decomposition Technique " Telecommunication computing Electronics and Control ISSN 1693-6930 Volume 15, Number 4 (2017), pp. 1750-1756

[6] G. S. C. Kumar, D. Prasad, V. S. Rao and N. R. Sai, "Utilization of Nominal Group Technique for Cloud Computing Risk Assessment and Evaluation in Healthcare," 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), 2021, pp. 927-934, doi: 10.1109/ICIRCA51532.2021.9544895

[7] V. S. Rao, V. Mounika, N. R. Sai and G. S. C. Kumar, "Usage of Saliency Prior Maps for Detection of Salient Object Features," *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2021, pp. 819-825, doi: 10.1109/I-SMAC52330.2021.9640684

DOI: 10.36893.DRSR.2023.V13I04.0036-0039