IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657
Volume 5,Issue 2,April 2017

APPLICATION OF CHAOTIC BLOCKCHAIN ALGORITHM FOR EFFICIENT DIGITAL CERTIFICATE VALIDATION

Dr.Y. V.Ram Kumar,B. Srinivas,T. Nirosh Kumar,Chandra Sekhar K

ABSTRACT: In the digital world, each and everything is digitalized in which the certificate of SSLC, HSC, and academic certificate are digitalized in the educational institution and provided to the students. Students are difficult to maintain their degree certificates. For the organization and institution, verification and validation of certificates are tedious and cumbersome. Our project will help to store the certificate in the blockchain system and provide security. First, the paper certificates are converted into digital certificates. The chaotic algorithm is used to generate the hash code value for the certificate. Then the certificates are store in blockchain. And these certificates are validated by using the mobile application. By using blockchain technology we can provide a more secure and efficient digital certificate validation.

1. INTRODUCTION

Block chain was introduced in the year 2008 by Satoshi Nakamoto. Block chain is one of the online ledgers which provide decentralized and transparent data sharing. In this project, we design an android application used to provide secure verification of our certificates. In nowadays, all Graduation certificates and transcripts hold information that is easily tampered illegally by individuals and should not be easily accessible to outside entities. Hence, there is a high need for an efficient mechanism, that can guarantee the information in such certificates is original, which means the document has originated from a reliable and authorized source and is not forged. Various systems have been designed to secure e-certificates for education institutions and to store them securely in cloud-based systems. Blockchain is the main tool to felicitate this need and when combined with different hashing techniques, this becomes a powerful method for protecting the data. It also helps in eliminating the need for constant verification of certificates. Blockchain technology is used to reduce the incidence of certificate forgeries and ensure that the security, validity, and confidentiality of graduation certificates would be improved. Technologies that exist in security domains include digital signatures, which are used in digital documents to provide authentication, integrity, and non-repudiation. Also, with blockchain in play, the storage of certificates is more secure. With these technologies, an application created that facilitates the secure validation of digital certificates.

Department of CSE, PRAGATI Engineering College(Autonomous),
Surampalem, A.P, India.

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657
Volume 5,Issue 2,April 2017

RELATED WORKS

Jin-chiou et al [1] developed software in order to avoid counterfeiting certificates. Due to the lack of an anti-forge mechanism, the graduation certificate is to be forged. so, the decentralized application was designed based on etherum blockchain technology. First, generate the digital certificate for the paper certificate then hash value created for the certificate is stored in the blockchain system. Even it used to verify the authenticity of the certificate it required another scanning app to scan the certificate. The system saves on paper, prevent document forgery. But the QR- Code must be scanned with a smartphone and an internet connection is required.

Ze Wang et al [2] designed a blockchain-based certificate transparency and revocation transparency system. In this system, the certificate authority (CA) signed the certificate and the revocation status information of the respected certificates are published by the subject (Certificate Authority). Public logs are used to monitor the Cas operation. This system was implemented with Firefox and nogix. This system provided the trust but Certificate validation is delayed and a false sense of security.

Madala et al [3] used the Hyper ledger Fabric blockchain platform. In this system, the certificates are issued by CAs only by obtaining approval from the domain owner Certificate Transparency (CT) technique, invented by Google. The aim to prevent SSL/TLS CA from issuing certificates for a domain without visible to the owner of the domain. But there was low scalability and lesstransaction.

Aisong Zhang et al [4] designed a system based on consortium blockchain technology. They used a secret sharing scheme. It can validate the digital certificate to protect the user's information and also the property of the user. The digital certificate revocation lists have collaborated among the CAs. The trust and reliable CRL (Certificate Revocation List) are more compared with thetraditional system. If the user wants to verify the certificate, they only need to decrypt the signature with the public key. And the result will be compared with the hash operation of the original message. If the result is consistent, it proved that the digital certificatenot tampered. But there is a false sense of security.

Macro Baldi etal[5] designed a system named certificate validation through public ledgers and blockchain. In this system, CRLs(Certificate Revocation List) were distributed through the use of a private blockchain, and it shared among CA(certificate authority).CAs are responsible for issuing certificates to requestors who meet the requirements and maintain CRLs. The certificate revocation list was available and authentication was provided at any time for a certificate. The certificate revocation list for a set of the certificate was maintained by the same certification authority who issued the certificates? CA ecosystem is fragile and prone to compromise.

III. OBJECTIVES OF THE PROPOSEDSYSTEM

By using the unmodifiable property of blockchain provide more security. Confidentiality is transparent with each transaction visible to all the peers. Our application runs in offline mode. The certificate is validated rapidly. Provide accurate and reliable information.

IV. PROPOSED SYSTEM

A. Methodology

In this proposed system the academic, sports certificates are converted into digital certificates using sampling and

ISSN 2347–3657
Volume 5,Issue 2,April 2017

quantization. Then the certificates are added with the hash values generated for the digital certificate and store it into the blocks. The chaotic algorithm used for generating the hash value. Each block consists of the hash value, timestamp, and hash value of the previous block. These blocks are linked together in the form of blockchain. The institution registers the student details in our interface (application) by providing details like name, email id and these are stored in the database. The certificate issued by the registrar is stored in the application and they form a blockchain. The employer or verifier can validate the certificate by entering the student details.

B. Digital Certificate Creation

In this, the student certificates are converted into digital certificates. The academic certificate and sports certificate are issued by the institution are stored in the database. By using the analog image to digital image conversation method, the certificate can be converted into a digital certificate. The value 0's and 1's are created for each certificate. In a digital image, all the coordinates on 2-d function and the corresponding values are finite. Each value considered a pixel. By using admin login, the administrator login to our application to upload the student's certificate in the application then it will convert an analog image to digital image using sampling and quantization. The next page of the application shows the add student and add a certificate. If an admin tape the add student, the new student gets registered. If an admin clicks the added certificate, the student certificate is uploaded.

C. Hash Code Generation

The chaotic algorithm is used to generate the hash value for the certificate. This algorithm takes input in different size and produces the output in a fixed size. This algorithm needs to define the mapping scheme, initial condition, and parameters. Verifying process is started by using the same initial condition and parameters to generate the same output. Whenthe certificate is uploaded, the hash value is created for the digital certificate. Compared to SHA-1, the chaotic hash function are collisionresistant.

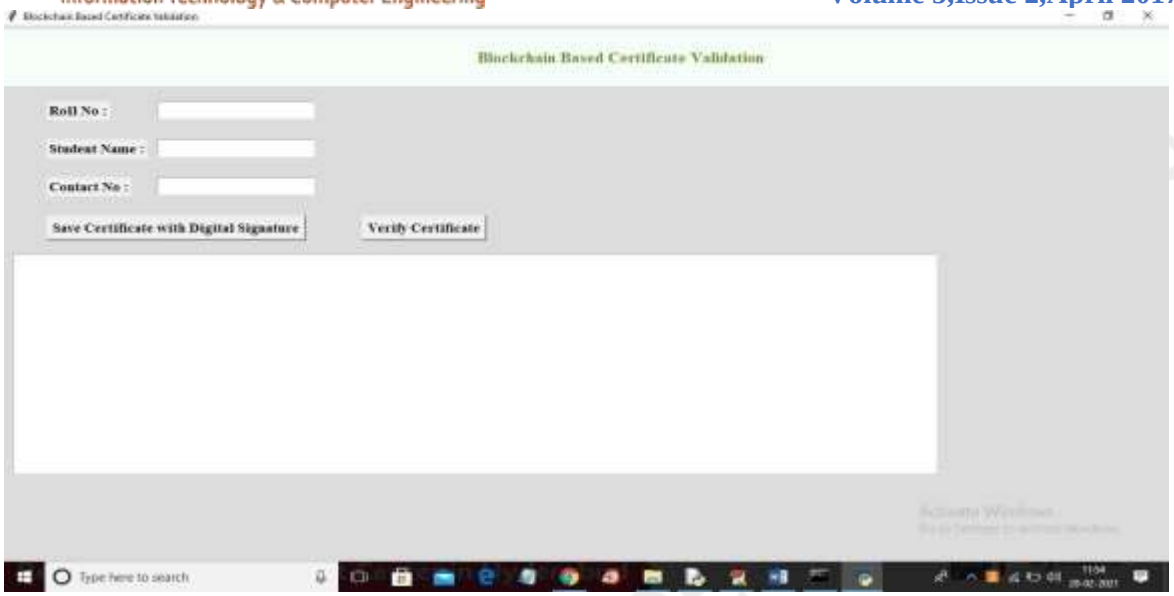
D. Digital certificate validation

In this, the created digital certificate is validated. Certificates that are stored in the blockchain are validated by matching the hash value. The verification of the hash value of the certificate is used to avoid tampering. The employer or verifier can log in to the application using their login id and password. They can select and certificate type which they want to validate. Then tape the validate button in the application. If the certificate is original the output will be a valid certificate and success. If the certificate is not original or modified the output will be error and modified certificate.

E. Working of Application

In our application the first page is home page consists of add certificate and last verifier page. Then the admin can add the student and their certificates by tap the add student and add certificate button. Next, the verifier can validate the certificate using the verifier login id and password. They provide the certificate and select the certificate type and tap the verify button. If the uploaded certificates are original then the result will bea success. Otherwise, the result will be error and modified.

International Journal of
Information Technology & Computer Engineering
ISSN 2347–3657
Volume 5,Issue 2,April 2017



In above screen enter student details and then click on 'Save Certificate with Digital Signature' button to convert certificate into digital signature and then saved in Blockchain.

In above screen entered some student details and then click on 'Save Certificate with Digital Signature' button and then selecting and uploading '1.jpg' file and then click on 'Open' button to get below screen.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 5,Issue 2,April 2017

In above screen we can see Blockchain generated previous hash with block no 1 and its current hash and then keep on generating new blocks with each certificate upload and while running you can see that previous hash of new record will get matched with current hash of old record and this matched hash code proof that Blockchain verify old and new hash code before storing new block to confirm data is not altered. So above details stored at Blockchain and now verifier can click on 'Verify Certificate' button and upload same or other images to get below result.

In above screen we uploaded same and correct image so application matched digital signature and then retrieve details from Blockchain and now try with some other image

In above screen verification got failed as uploaded certificate not matched with stored certificates in Blockchain. Similarly, you can upload any other certificate and convert them to digital signature

ISSN 2347–3657
Volume 5,Issue 2,April 2017

V. CONCLUSION

In this paper, we proposed a solution to the problem of certificate forgery based on blockchain technology. Providing security to the data is very important. By using the unchallengeable property of blockchain, we can provide more security for data and reduce the certificate forgery. The application can allow the user to view and validate the certificate. This system guarantees information accuracy and security and easy for people to manage digital certificates.

11.REFERENCES

VI. 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 June2018, Suzhou.

[4] P. H. Arnoux, A. Xu, N. Boyette, J. Mahmud, R. Akkiraju, V. Sinha, "25 Tweets to Know You: A New Model to Predict Personality with Social Media", International AAAI Conference on Web and Social Media, 16-18 May 2017, Montreal, Canada, 2017.4.

A. Abdelrazeq et al., "Sentiment Analysis of Social Media for Evaluating Universities," Proc. 2nd Int'l Conf. Digital Information Processing, Data Mining, and Wireless Comm. (DIPDMWC 15), 2015, pp. 49–62. [5]Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi "Certificate Validation through Public Ledgers and Blockchains In Proceedings of the First Italian Conference on Cybersecurity.

[6] Nitin Kumavat, Swapnil Mengade, Dishant Desai, JesalVarolia, "Certificate Verification System using Blockchain" Computer Engineering Department, Mumbai University.

[7] S.Sunitha kumari, D.Saveetha "Blockchain and Smart Contract for Digital Document Verification" Department of Information Technology- SRM Institute of Science and Technology.

[8] Omars Saleh, osman ghazali, muhammad ehsan rana, "Blockchain based framework for educational certificates verification" Studies, Planning and Follow-up Directorate, Ministry of Higher Education and Scientific Research, Baghdad, Iraq. School of Computing, University Utara Malaysia, Kedah, Malaysia.

[9] Trong Thua Huynh, Trung Tru Huynh, Dang Khoa Pham, Anh Khoa Ngo, "Issuing and Verifying Digital Certificates with Blockchain" https://dx.doi.org/ 10.1109/ ATC .2018.8587428.

[10] Maharshi Shah, Priyanka Kumar, "Tamper Proof Birth Certificate Using Blockchain Technology" International Journal of Recent Technology and Engineering (IJRTE).

International Journal of
Information Technology & Computer Engineering

ISSN 2347–3657
Volume 5,Issue 2,April 2017