ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 7, Issue 7, July 2020

Privacy Preservation of Fraud Document Detection on Online Social Network

Mr.T.Anto Theepak
Assistant Professor, Department of Information Technology,
Francis Xavier Engineering College, Tirunelveli
K.Alfinn Sam Solomon, C.Athipan, C.Selvin John, K.Maharajan
UG Student, Department of Information Technology,
Francis Xavier Engineering College, Tirunelveli

Abstract: Prevention of fraud and abuse has become a major concern of many organizations. The best way to reduce frauds, fraudsters are adaptive and will usually find ways to circumvent such measures. Detecting fraud is essential once prevention mechanism has failed. Several cryptographic algorithms have been developed that allow one to extract relevant knowledge from a large amount of data like fraudulent financial statements to detect. In this project present an efficient approach for fraud detection on scanned government documents and government certificates such as community certificates, Birth certificates, Native Certificates, Income certificates, students Transfer certificate, Mark Sheet etc. In this approach was first maintain the scanned certificates by the administrator. Then the encrypt data by SHA algorithm and save it into the database. Here generate the hash key for encryption which is created by our given data. Block chain technology is used to maintain the records. Every record has its own hash key, encrypted data and previous hash key, previous encrypted data. If any government certificate is modified, the hash key is automatically changed. Then block chain validation is failed. The block chain is automatically recover the modified data from its previous encrypted data. This project is developed using PHP as front end and MySQL as back end.

I. INTRODUCTION

Prevention of fraud and abuse has become a major concern of many organizations. The industry recognizes the problem and is just now starting to act. Although prevention is the best way to reduce frauds, fraudsters are adaptive and will usually find ways to circumvent such measures. Detecting fraud is essential once prevention mechanism has failed. Several cryptographic algorithms have been developed that allow one to extract relevant knowledge from a large amount of data like fraudulent financial statements to detect. In this work we present an efficient approach for fraud detection on scanned documents/certificates such as Transfer certificate, mark sheet etc. This work presents a detection scheme for a fraudulent document made by image. The fraud document is indistinguishable by the naked eye from a genuine document because of the technological advances. Even though we cannot find any visual evidence of forgery, the fraud document includes inherent device features. We propose a method to detect fraud documents "Block chain methodology". The scope of this system is used to detect the distortion of the document on the fake documents, so they developed an approach to identity the static parts of the documents. This system compares the two images together and computes the matching score. This matching score can be considered as a number identical character that has the same position or a different one. However, we see that it will be a stronger authentication if they include the non-static part in the authentication, by font recognition or printer type.

II. LITERATURE SURVEY

In smart grid systems, secure in-network data aggregation approaches have been introduced to efficiently collect aggregation data, while preserving data privacy of individual meters. Nevertheless, it is also important to maintain the integrity of aggregate data in the presence of accidental errors and internal/external attacks. To ensure

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 7, Issue 7, July 2020

the correctness of the aggregation against unintentional errors, we introduce an end-to-end signature scheme, which generates a homomorphic signature for the aggregation result. The homomorphic signature scheme is compatible with the in-network aggregation schemes that are also based on homomorphic encryption, and supports efficient batch verifications of the aggregation results. Next, to defend against suspicious/compromised meters and external attacks, we present a hop-by-hop signature scheme and an incremental verification protocol. In this approach, signatures are managed distributed and verification is only triggered in an ex post facto basis - when anomalies in the aggregation results are detected at the collector. The loosely defined terms hard fork and soft fork have established themselves as descriptors of different classes of upgrade mechanisms for the underlying consensus rules of (proof-of-work) block chains. Recently, a novel approach termed velvet fork, which expands upon the concept of a soft fork, was outlined in [22]. Specifically, velvet forks intend to avoid the possibility of disagreement by a change of rules through rendering modifications to the protocol backward compatible and inclusive to legacy blocks. We present an overview and definitions of these different upgrade mechanisms and outline their relationships. Hereby, we expose examples where velvet forks or similar constructions are already actively employed in Bitcoin and other cryptocurrencies. Furthermore, we expand upon the concept of velvet forks by proposing possible applications and discuss potentially arising security implications. Blockchain is an emerging technology for decentralised and transactional data sharing across a large network of untrusted participants. It enables new forms of distributed software architectures, where agreement on shared states can be established without trusting a central integration point. A major difficulty for architects designing applications based on blockchain is that the technology has many configurations and variants. Since blockchains are at an early stage, there is little product data or reliable technology evaluation available to compare different blockchains. In this paper, we propose how to classify and compare blockchains and blockchain-based systems to assist with the design and assessment of their impact on software architectures.

III. THEORY

The graduation certificates issued by universities and other educational institutions are among the most important documents for graduates. A certificate is a proof of a graduate's qualification and can be used to apply for a job or other related matters. The advance of information technology and the availability of low-cost and high-quality office equipment in the market have enabled forgery of important documents such as certificates, identity cards, and passports. However, verification of certificates using traditional methods is costly and very time-consuming. In order to solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be proposed. By the unmodifiable property of blockchain, the digital certificate with anti-counterfeit and verifiability could be made. In this paper purposed Blockchain can be considered as the next generation of cloud computing, and is expected to radically reshape the behaviour model of individuals and organizations, and thus realize the transition from the Internet of Information today to the future Internet of Value. Blockchain is a distributed database that is widely used for recording distinct transactions. Once a consensus is reached among different nodes, the transaction is added to a block that already holds records of several transactions. Each block contains the hash value of its last counterpart for connection. All the blocks are connected and together they form a block chain. Data are distributed among various nodes (the distributed data storage) and are thus decentralized. Consequently, the nodes maintain the database together. Under block chain, a block becomes validated only once it has been verified by multiple parties. Furthermore, the data in blocks cannot be modified arbitrarily. A block chain-based certificate, for example, creates a reliable system because it dispels doubts about information's veracity.

ADVANTAGES OF PROPOSED SYSTEM

- Block verification and production - Security
- Speed and Accuracy

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 7, Issue 7, July 2020

- Node verification and Increase the block - Efficiency and flexibility
- Enhance the Security
- Private key sign
- Public broadcasting

IV. Experiments And Results

Digital uses are now the norm and the benefits to be gained by organisations are considerable: acceleration of transactions, automation or do-it-yourself approaches favour a rapid Region of Interest. However, the digitalisation of documents and their attachments is fundamental for all processes, and easy access to image retouching tools, also simplifies their falsification. As a result setting standardised digital processes for fraud, is becoming a strategic challenge for companies seeking to simplify their customer and supplier relations while avoiding the malicious behaviour that can be costly for companies (both financially and concerning brand image). The fraud document detection is needed for following areas. For example, healthcare fraud, which has been estimated at more than billion by the Indian Healthcare Fraud & Corruption Network. This is why any project of digitalisation and automation of processes can no longer be considered independently of a powerful system of automatic fraud detection.

V. Conclusion

Verification of the job related documents are time consuming and cost extensive. In addition, companies usually had to rely on third party for the verification process which sometimes become very cumbersome. In this project have shown how blockchain technology can be used to overcome those limitations. Have to proposed an architecture for blockchain based work history validation. This allows the individuals to share their work history and employers to verify the data. The employed smart contact to ensure the privacy of the individuals. Finally, They have shown the implementation of our proposed architecture using Ethereum based public blockchain. If such system is adopted by the employers, then work history related fraud can be reduced.

VI. Future Scope

For future work, the proposed model will be implemented and adopted in selected educational institutions. It will be further extended to be based on smart contracts. The blockchain technology that has greatly improved the global economy since it is possible for parties to trust each over a long distance through the blockchain records and be able to conduct business operations suitably. It is important to be more facilitated on its numerous operations to achieve better future for currency transaction and improve trust amongst business operators.

References

[1]. Li F, Luo B. Preserving data integrity for smart grid data aggregation. InSmart grid communications (SmartGridComm), 2012 IEEE third international conference on 2012 Nov 5 (pp. 366-371). IEEE.

[2]. Kumar RS, Saxena A. Data integrity proofs in cloud storage. In Communication Systems and Networks (COMSNETS), 2011 Third International Conference on 2011 Jan 4 (pp. 1-4). IEEE.

[3]. A Wild Velvet Fork Appears! Inclusive Blockchain Protocol Changes in Practice: FC 2018 International Workshops, BITCOIN, VOTING, and WTSC, Nieuwpoort, Curaçao, March 2, 2018, Revised Selected Papers

[4]. Liang X, Shetty S, Tosh D, Kamhoua C, Kwiat K, Njilla L. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing 2017 May 14 (pp. 468-477). IEEE Press.

[5]. Ramachandran A, Kantarcioglu D. Using Blockchain and smart contracts for secure data provenance management. arXiv preprint arXiv:1709.10000. 2017 Sep 28.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 7, Issue 7, July 2020

[6]. Pilkington M. 11 Blockchain technology: principles and applications. Research handbook on digital transformations. 2016 Sep 30:225.

[7]. Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. InSecurity and Privacy (SP), 2016 IEEE Symposium on 2016 May 22 (pp. 839-858). IEEE.

[8]. Xu X, Weber I, Staples M, Zhu L, Bosch J, Bass L, Pautasso C, Rimba P. A taxonomy of blockchain-based systems for architecture design. InSoftware Architecture (ICSA), 2017 IEEE International Conference on 2017 Apr 3 (pp. 243-252). IEEE.