

BLOCK CHAIN BASED VERIFICATION AGAINST PROCRASTINATING AUDITORS

AASIFA K¹, BHARATHI B², KEERTHI V³, M.SAMUNDEESHWARI⁴

¹ UG Scholar, Department of CSE, Kingston College, Vellore-59

² UG Scholar, Department of CSE, Kingston College, Vellore-59

³ UG Scholar, Department of CSE, Kingston College, Vellore-59

⁴ UG Scholar, Department of CSE, Kingston College, Vellore-59

Abstract—Sending Distributed Storage Administrations has key benefits in managing information for customers. Anyway, it also comes with a lot of security issues and one of them is the accuracy of the information. Open verification methods can allow a client to use an external evaluator to confirm the honesty of the information to the benefit of the organization, while existing open confirmation plans are vulnerable examiners who may not perform confirmations accurately. In this document, we propose a delegated third-party auditor for the background check process performed by each organization.

A new verification mode has been introduced in our project which implements block chain technology. By usage of block chain each and every data about the candidate which is available in the database will remain secured. We use this technology to access past related data about a candidate who will be verified by the auditor, by providing a unique identity for each entity involved in the verification process. Once the process is complete, the auditor will update the results statement in database and then the candidate will be available to the organization for further process. By the usage of this block chain technology the background details of the persons will be stored in a confidential manner.

Key Words: security issues, verification mode, block chain technology

1. INTRODUCTION

Checking people's surroundings and citations may take time. It can be a slow process and expensive. Prospective employees often stretch the truth on applications or fail to fill out all of the information you need to make a decision. They may not sign off on authorization forms which slows you down. Certifications and qualifications can be falsified as can ID. Employment histories are often incomplete, inaccurate, or misleading. Too many hiring managers take shortcuts when hiring people because they are blinded by the candidate's resume or performance during the interview phase. They may skip hiring certification validation or employment verification.

Just because someone interviews well doesn't mean they will be a great enroll. To make sure candidates provide accurate information you can trust, it takes time. Employers can't impart to make mistakes. Hiring certification validation or employment verification is critical to avoid making bad hires. The block chain process helps both employers and job seekers. It allows for faster filtering of candidates and lets you make hiring decisions based on verified information. For candidates, it can simplify the application process and give them a competitive advantage over other applicants. This advantage gives candidates an incentive to participate and make sure all information is accurate.



Figure 1: Block chain verification

2. RELATED WORKS

[1] This work done by L Zhong, Q Wu, J Xie, J Li, B Qin "A secure versatile light payment system based on block chain" in the year 2019.

Ever-increasing transaction costs, serious network congestion, and low transaction rates in the current block chain systems restrict their extensive use. To relieve from this situation, we present a secure versatile light payment (SVLP) scheme. The SVLP merely employs a digital signature algorithm and a one-way function and has similar security comparing to existing blockchain systems, such as Bitcoin and Ethereum. The proposed scheme is of ultra-low power consumption, since the payers and payees only need one-way functions to achieve multiple transactions, instead of the

costly digital signature algorithms. Furthermore, the processes of payment and refunding are flexible. This is due to the fact that the denomination in our scheme possesses divisibility and the users need not to verify the pre images on the long chain one-by-one. Finally, as the transaction can be taken off-chain and offline, it can be even used in remote areas or geological disasters areas where communication infrastructures are lacked or destroyed. All these features indicate that our scheme is practical and versatile.

[2] This work done by G. Xu, H. Li, Y. Dai, K. Yang and X. Lin “: Enabling efficient and geometric range query with access control over encrypted spatial data” in the year 2019

As content is transmitted in content-driven manner in the content-centric network (CCN), it does not require any host address; therefore, it is infeasible to establish a traditional secure channel between hosts. Securing the content transmission in the CCN is a challenging problem. We solve this problem with the content-based encryption, where the encryption key is associated with the content itself, and the private decryption keys are distributed to the authorized consumers. To deal with the security requirements for content-based encryption, we define a security model that captures the key existential unforgeability and semantic security. We then propose a content-based encryption scheme with short ciphertexts, which is proven to be strong key existentially unforgeable and semantically secure in the standard model. We apply the scheme to construct a secure content transmission protocol in the CCN, which captures the security properties of content confidentiality, integrity, resistance to replay attacks and resistance to key forgery attacks. The performance analysis shows that our protocol is efficient for large content transmission

[3] This work done by Xuemin Sherman Shen, Cheng Huang, Dongxiao Liu, Liang Xue, Weihua Zhuang, Rob Sun, Bidi Ying “Data Management for Future Wireless Networks: Architecture Privacy Preservation and Regulation” in the year 2021.

Next-generation wireless networks (NGWN) aim to support diversified smart applications that require frequent data exchanges and collaborative data processing among multiple stakeholders. Data management (DM), including data collection, storage, sharing, and computation, plays an essential role in empowering NGWN. However, DM for NGWN faces two significant challenges: stakeholders' data cannot be easily managed across different trust domains under a distributed network architecture; and privacy preservation requirements of personal data become more rigorous under new privacy regulations. To explore possible solutions to address the challenges, we first

investigate the state-of-the-art architecture designs for DM and emphasize advantages of a blockchain-based DM architecture. Then we summarize existing privacy-preserving techniques in terms of advantages and challenges when being applied to DM. In addition, we review recent privacy regulations with their impacts on DM and discuss the existing solutions with privacy regulation compliance based on block chain. Finally, we identify further research directions for achieving DM with privacy preservation.

3. PROPOSED SYSTEM

The proposed system defeats the problem of existing scheme by giving a verification scheme which is destined by the auditor. It consists of two phases, in the first phase, the auditor checks the unification of deployed data which is the data provided by the data provider/user. The deployed data is in the second phase, the auditor uses the connected data in the block chain and the verification is done by retrieving the information and perform matching operation between the data where each verification executed by the auditor only, and it is consolidated by the block chain. The main idea is to require auditors to record each verification outcome into a database. The actual data of the system will be kept in the organization once it is verified. And recovery of the chain is based on the key identification from the information provided by user.

3.1 ADVANTAGES OF PROPOSED SYSTEM

- Malicious activities will be restricted by using the auditors.
- User data is stored and maintained by the use of Block chain by unique ID.
- Verification overhead on many data will be minimized.
- Management of the data integrity will be optimized.
- Users privacy data will be protected even if there is a misleading entity

3.2 ALGORITHM

3.2.1 SHA-512

SHA-512 is the abbreviation of Secure Hash Algorithm 512, is a hashing set of rules used

to convert textual content of any period right into a fixed-length string. Each final results produces a SHA-512 period of 512 bits (sixty four bytes). This set of rules is regularly used for e mail addresses hashing, password hashing, and virtual document verification. SHA-512 is likewise utilized in blockchain technology, with the maximum notable instance withinside the BitShares network. It moderates the layout and management of addresses, and is likewise used for transaction verification.

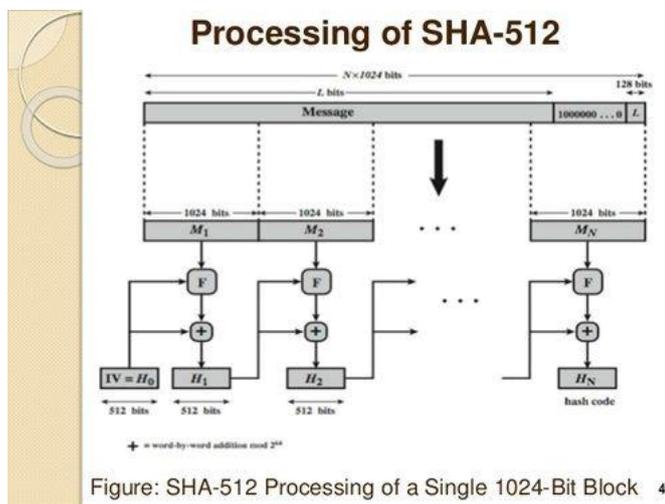


Figure: SHA-512 Processing of a Single 1024-Bit Block 4

Figure 2: Processing SHA-512

3.3 MODULE DESCRIPTION

3.3.1 MODULE 1: CANDIDATE

The employee module contains the Details uploaded to the Auditor for the verification process performed by the auditing entity. The candidate needs to provide the data for verification before entering to the organization. There is background verification process must happen at the point of entry. For that purpose the candidate should submit the original details to the auditor for further process

3.3.2 MODULE 2: KEY GENERATION

The key generation center is responsible for the generation of initial public key for the candidate to upload the details. Once the candidate register with the application the key generation center is responsible to send the unique key for further including of the employee details into the block chain technology.

3.3.3 MODULE 3: AUDITOR

An auditor is the responsible entity which handles the verification process in time, with the data that stored in the centralized database. The auditor having the authority to retrieve the data presented in the database as block chain format. So that each and every data about the candidate is contained in the database remains more secured.

3.3.4 MODULE 4: ADMINISTRATOR

The administrator module handles the overall maintenance of the authentication to be given to the auditors as well as to the candidates. And the administrator can able to view the auditors even if the auditor execute the verification accurately. And the overall maintenance of the application is verified by the admin.

4. ARCHITECTURAL AND DATA FLOW DIAGRAM

4.1 ARCHITECTURAL DIAGRAM:

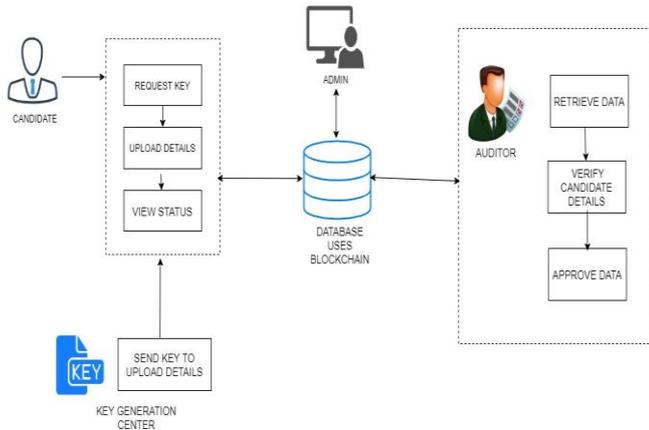


Figure 3: Architectural Diagram

The architecture diagram of proposed is given above. The components present in it are candidate, key generation, auditor, administrator and process runs between them with the database to verify the information.

4.2 DATA FLOW DIAGRAM:

In the current physical data flow diagram, the process label includes the names of people or their locations or the names of computer systems that provide the overall system processing label include an identification of the technology used to process the data in the computer system. Similarly, data flows and data stores are often labeled with the names of the actual physical avenue on which data such as folders, computer files, data forms or computer rolls are stored.

4.2.1 CURRENT LOGICAL:

The physical aspects in the system are removed as much as possible so that the system is reduced to its essence to the data and the processes that changes them regardless of the current physical format.

4.2.2 PREVIOUS LOGIC:

This is the same as the current logical model if the user was completely satisfied the user was completely joyful with the functionality of the present system, but had issues with how it generally worked in the new logical model will differ from the current logical model while having add-up functions, entire functional remove and inefficient flows recognized.

Level 0

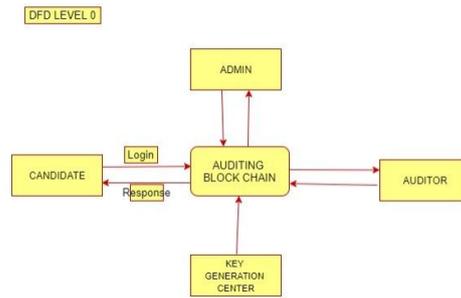


Figure 4: DFD Level – 0 diagram

Level 1

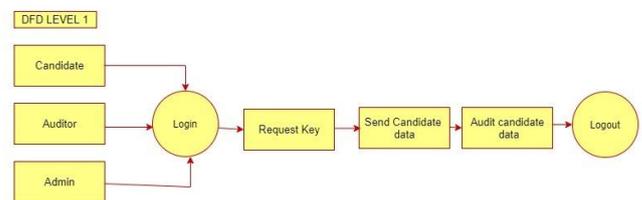


Figure 5: DFD Level – 1 diagram

Level 2

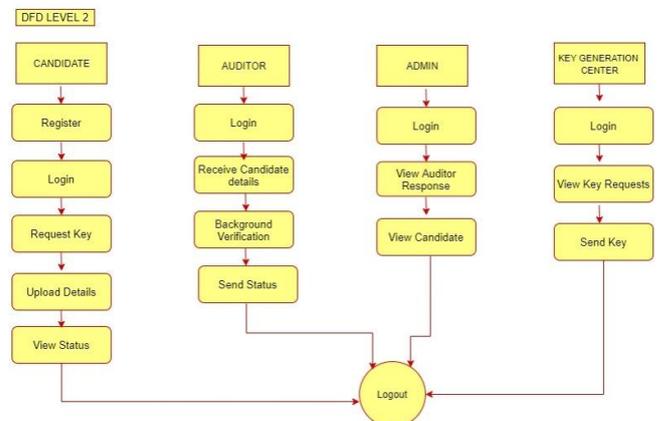


Figure 6: DEF Level – 2 diagram

5. RESULTS AND OBSERVATION

- It is an verification scheme for securing the information from procrastinating auditors and tampering of data so we can secure data using block chain technology.
- we have induced two step verification . A third party auditor who checks ,verifies the data and generates the key, where the key is sent to the users for security

DATASET 1:

REQUEST KEY

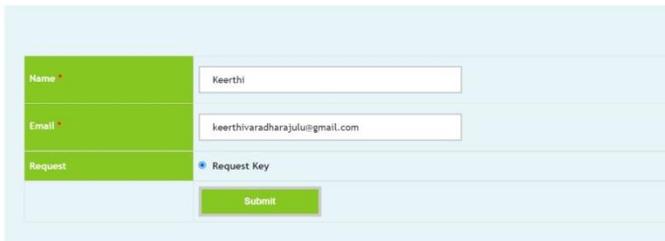


Figure 7:

DATASET 2:

SEND KEY

S.NO	NAME	EMAIL	PAN ID	REQUEST TYPE	DATE	STATUS
1	Keerthi	keerthivaradharajulu@gmail.com	HPKIE992N	Requesting_Key	24-05-2022	KEYSENT

Figure 8:

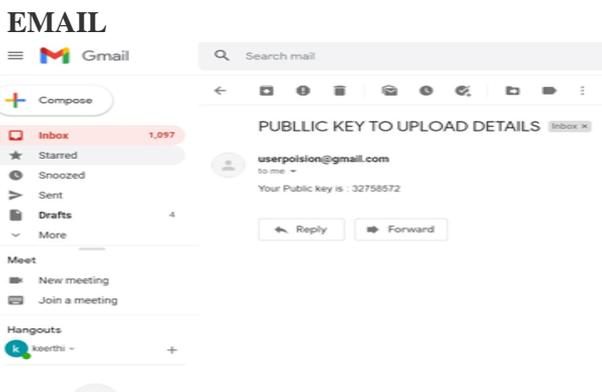


Figure 9:

AUDIT STATUS

AUDIT RESPONSE

NID	UPLOADED DATE	STATUS	RESPONDED DATE
EPK6932N	24-05-2022	PENDING	-

Figure 10:

AUDIT RESULTS

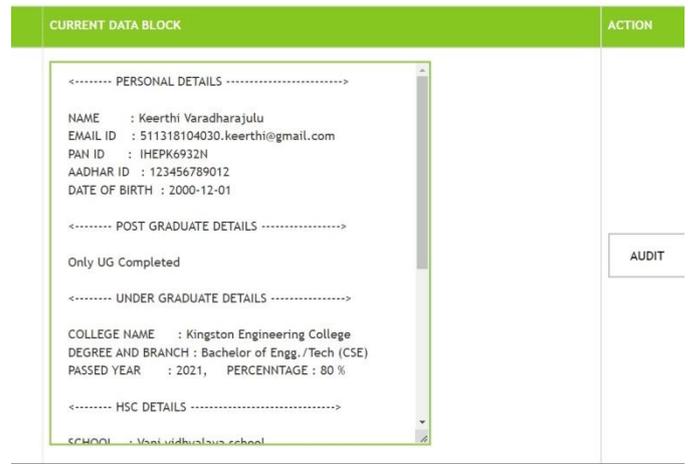


Figure 11:

AUDIT FINAL RESULTS

CANDIDATES LIST

PAN ID	DATE	STATUS
IHEPK6932N	24-05-2022	APPROVED

Figure 12:

5.1 OBSERVATIONS

- In data set 1 the user logs in the page by registering after logging in they will request a key from the admin . The admin sends the key through their mail id after receiving the key the users have to upload their details .
- In dataset 2 The auditor generates the key and verifies the user's information if it is accurate then they will be approved by the auditor.

6 CONCLUSION

we proposed a verification scheme on the outsourced data of the candidate by the recognized auditor delegated by the organization. It utilizes the chain properties, where each verification performed by the auditor is integrated into the Block chain. The analysis demonstrates that it provides the security with existing schemes of data verification. In the comprehensive performance analysis, this demonstrates that the it has constant communication overhead and is efficient in terms of computation overhead. We will also investigate how to utilize Block chain technology to enhance the auditing system in terms of security, performance, and functionality.

ACKNOWLEDGEMENT

The authors would like to thank Mrs.M.SAMUNDEESHWARI for her suggestions and excellent guidance throughout the project period.

REFERENCES

- [1] J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, "Privacy-preserving data aggregation computing in cyber-physical social systems," *ACM Transactions on Cyber-Physical Systems*, vol. 3, no. 1, p. 8, 2018.
- [2] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in internet of things with privacy preserving: Challenges, solutions and opportunities," *IEEE Network*, vol. 32, no. 6, pp. 144–151, 2018.
- [3] J. Li, H. Ye, W. Wang, W. Lou, Y. T. Hou, J. Liu, and R. Lu, "Efficient and secure outsourcing of differentially private data publication," in *Proc. ESORICS*, 2018, pp. 187–206.
- [4] L. Zhong, Q. Wu, J. Xie, J. Li, and B. Qin, "A secure versatile light payment system based on blockchain," *Future Generation Computer Systems*, vol. 93, pp. 327–337, 2019.
- [5] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, "Enabling efficient and geometric range query with access control over encrypted spatial data," *IEEE Trans. Information Forensics and Security*, vol. 14, no. 4, pp. 870–885, 2019.
- [6] K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. Shen, "Privacy-preserving attribute-keyword based data publish-subscribe service on cloud platforms," *Information Sciences*, vol. 387, pp. 116–131, 2017.
- [7] W. Shen, B. Yin, X. Cao, Y. Cheng, and X. Shen, "A distributed secure outsourcing scheme for solving linear algebraic equations in ad hoc clouds," *IEEE Trans. Cloud Computing*, to appear, doi: 10.1109/TCC.2016.2647718
- [8] H. Yang, X. Wang, C. Yang, X. Cong, and Y. Zhang, "Securing content-centric networks with content-based encryption," *Journal of Network and Computer Applications*, vol. 128, pp. 21–32, 2019.
- [9] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in *Proc. of ESORICS*, 2009, pp. 355–370.
- [10] X. Zhang, H. Wang, and C. Xu, "Identity-based key-exposure resilient cloud storage public auditing scheme from lattices," *Information Sciences*, vol. 472, pp. 223–234, 2018