Al-Farabi Journal of Engineering Sciences Volume (4), Issue (2) December (2025)

ISSN: 2617-5517 (issn.org)
Al-Farabi Journal of Engineering Sciences
https://iasj.rdd.edu.iq/journals/journal/view/97
مجلة الفارابي للعلوم الهندسية تصدرها جامعة الفارابي

Enhancing HR Payroll System Management with Blockchain Technology

Ali H. Kashmar[1],Ammar I. Shihab[2], Wafaa S.Jawad[3]

[1]Department of Cyber Security, College of Science, Al-Farabi University, Baghdad, Iraq.

[2]Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq.

[3]Dep. of Computer and Communication, Faculty of Engineering, Islamic University of Lebanon, Beirut,Lebanon

Corresponding author: Ali H. Kashmar, ali.habib@alfarabiuc.edu.iq

Abstract

This paper contributes to the advancement of blockchain technology in the financial sector and sets a new standard for payroll management in the digital identities, proposed model involves: data generation, encryption, blockchain creation, and summary reporting. Create fake datasets by bootstrap and create good-looking XML documents and datasets has been created for 25000 records. Each record has (‘id', 'name', 'sex', 'birthdate', 'certificate', 'title', 'department', 'level', and 'salary'). Read datasets in the model and generate unique key generator has been calculated by lower key size, upper key size, digits, and punctuation. Generate random characters for each category without duplicates, combine all categories into a single list, shuffle the list to randomize the characters, and then convert the shuffled list back to a string and return it as the AES key. The model has been tested by National Institute of Standards and Technology (NIST). Results show that the model working perfectly, therefore show the model was successfully passed with 12 features and fall with 3 features, mean that 80% passed 20% fall, thus test has been done under key encryption test. Otherwise, model has been tested on cipher text, and the result show that the model was successfully passed with 11 features and fall with 4 features, the percentage of successfully was 74% and fall in 26% in Figures (5.1) and (5.2) shows the test of model.

Keywords: *HR Payroll System, Blockchain Technology, NIST*

1. Introduction

The implementation of a blockchain-based automated payroll system presents a highly innovative option with the capacity to fundamentally transform conventional payroll procedures inside organizational contexts [1]. The revolutionary technology offers the potential to address the constraints of traditional payroll systems and revolutionize the way firms handle and distribute employee paychecks by removing manual interventions, optimizing workflows, and guaranteeing data integrity [2]. By leveraging blockchain technology, organizations can automate and enhance their payroll processes, resulting in a period characterized by remarkable efficiency, accuracy, and security. The exploration of blockchain-based payroll systems is leading to a notable transformation in the financial environment. This transformative process presents the potential to bridge current disparities and rectify the longstanding inadequacies that have impacted the industry [3]. The utilization of cryptographic algorithms in blockchain technology ensures a significant level of transparency, integrity, and security by recording each transaction as a block that is linked to previous ones [4]. In addition, the decentralized and secure characteristics of blockchain technology guarantee the confidentiality and protection of sensitive employee data, including salary information and personal details, by preventing unauthorized access [5]. The incorporation of blockchain technology into the management of payroll systems not only offers the potential for improved efficiency and security, but also establishes a foundation for a future in which trust and transparency play a dominant role in financial transactions [6]. The objective of this paper is to utilize the capabilities of blockchain technology in order to establish a payroll system that is secure, efficient, and transparent, while also automating the entirety of the payment process.

2. Related Work

[7], proposed framework of contemporary regulations, within the fundamental criteria for electronic document management typically encompass the utilization of electronic media for the storage and administration of corporate and other types of documents. [8], they encompassed several key components: a chain structure that facilitates data verification and storage, distributed consensus algorithms that enable the generation and updating of data, cryptographic techniques that ensure secure data transmission and access, and automated smart contracts that facilitate data programming and operations. This framework, which have termed the PDI model of blockchain security, allows for a systematic analysis of the various dimensions of security within the blockchain context. [9], they employ a consensus method among dispersed nodes to create and modify data. and delve into a comprehensive examination of the prevalent consensus processes employed in blockchain technology, while also conducting a detailed analysis of the concepts of anonymity and privacy preservation in the realm of digital currency. Their discourse has the potential to facilitate the advancement of Blockchain technology. [10], presents a novel approach that combines K-anonymity and searchable encryption techniques to provide a privacy-preserving scheme for sharing medical data among medical institutions and data users. [11], introduces a conceptual framework for the secure storage of data within a cloud computing environment. This framework employs smart contracts and access lists to ensure the security of data.

3. The Advanced Security in Blockchain Technology

Blockchain technology has the potential to provide a cohesive and decentralized platform for the secure recording, tracking, and management of various forms of information, including insurance details, proof of ownership, patents, repairs, maintenance, and tangible or intangible assets. The preservation of the accuracy and reliability of ledgers is a fundamental concern in the context of transactions involving actors within the automotive sector. The precision and immutability of blockchain technology play a crucial role in the enforcement of contractual relations in real-life scenarios, as well as in the prevention of improper practices and the effective management of the supply chain. In addition, the capacity to promptly retrieve authenticated data presents a multitude of possibilities and commercial frameworks, including the automation of operations via the Internet of Things (IoT) [12,13]. Blockchain technologies offer a robust level of security and trust that is essential for contemporary digital transactions. There exists a pervasive concern regarding the potential for individuals to exploit foundational software systems in order to manufacture counterfeit currency for personal gain. The blockchain technology employs three fundamental ideas, namely cryptography, decentralization, and consensus, to establish a robust software infrastructure that exhibits exceptional resistance to tampering. The presence of a single point of failure is absent, and the alteration of transaction data by a single user is not possible [14].

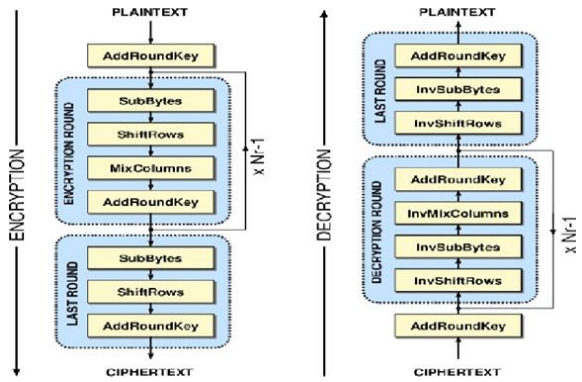


Figure (3. 1) Shows the basic AES-256 cryptographic architecture[15]

The utilization of the SHA-256 algorithm for authentication, along with the implementation of secure communication protocols, ensures the safeguarding of the key during the transmission process. The encryption algorithm utilized for storing the key is AES-256, whereas the authentication algorithm employed is SHA-256 [16]. In order to ensure the preservation of data integrity, an advanced encryption standard AES-256 encryption technology is employed for the encryption of data [17].

3.2 The National Institute of Standards and Technology (NIST)

In recent times, there has been a notable surge in the focus on cybersecurity management, mostly driven by the escalating frequency and gravity of cyberattacks, with a special emphasis on key infrastructures inside nations. The process of rapid digitalization has brought to light numerous vulnerabilities that possess a high potential for exploitation if not effectively handled. As a result, the European Union (EU) has enacted its inaugural cybersecurity directive, drawing inspiration from the Cybersecurity Framework developed by the US National Institute of Standards and Technology (NIST). This directive mandates that organizations responsible for vital infrastructure must engage in consistent monitoring and

reporting of their cybersecurity endeavors. Our study aimed to examine the extent to which the existing academic literature on cybersecurity metrics and controls encompasses the constituent functions outlined by NIST. Additionally, we sought to identify any discernible gaps in the coverage of these functions within the NIST framework. The analysis conducted yielded intriguing findings in both directions, indicating disparities within the academic discourse and regions that are not adequately covered within the NIST framework. It is our contention that forthcoming research ought to prioritize the identification, mitigation, and remediation of occurrences. Furthermore, the National Institute of Standards and Technology (NIST) stands to gain advantages by expanding its scope to encompass specific subject domains, including natural disasters, financial considerations, and organizational climate. The user has provided a numerical reference.

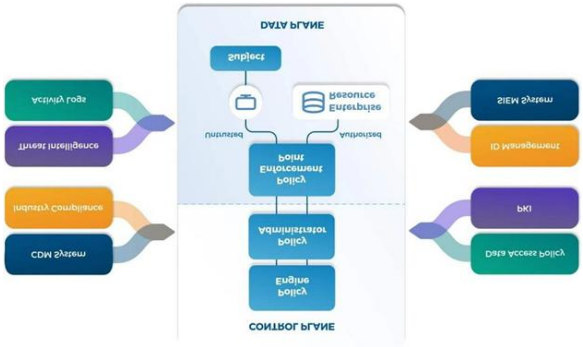


Figure (3. 2) Shows The NIST diagram [18]this group.

4. Research Methodology

Methodology of the proposed model in the paper that involves: “data generation, encryption, blockchain creation, and summary reporting”. Create fake datasets by bootstrap; datasets were created for 25000 records. Each record has (‘id', 'name', 'sex', 'birthdate', 'certificate', 'title', 'department', 'level', and 'salary'). Read datasets in the model and generate Unique key generator has been calculated by lower key size, upper key size, digits, and punctuation. Generate random characters for each category without duplicates, combine all categories into a single list, Shuffle the list to randomize the characters, then Convert the shuffled list back to a string and return it as the AES key

4.1 The General Workflow Steps

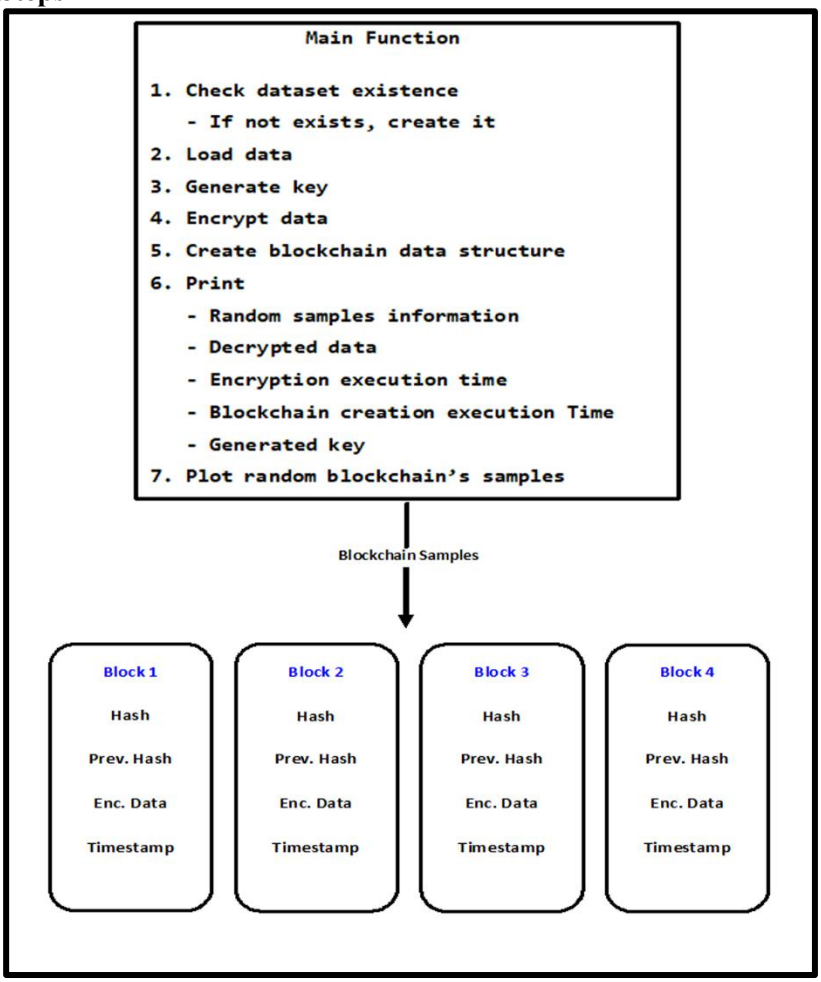


Figure (4.1) Shows the Structure of Blockchain Project Workflow Steps

4.2 Datasets

Datasets has been created by generate fake documentation, whether you need to bootstrap your database, create good-looking XML documents, and fill-in persistence to stress test it, or anonymizedata taken from a production service. Datasets has been created for ٢٥000 records. Each record have**('id', 'name', 'sex', 'birth-date', 'certificate', 'title', 'department' ,'level', and 'salary').**

Where:

Id created by Generate an ID (incremental) record['id'] = Len (data)+1

Generate a random first name and last name

record['name'] = fake. first_name () + " " + fake. last_name () +" " + fake. last_name () Generate a random sex (male or female)

record['sex'] = random. Choice (['Male', 'Female']) Generate a random birthdate within the specified age range

birth_year = random. Randint (1963, 2001) # Ages between 22 and 60 in 2023

record['birthdate'] = fake.date_of_birth(tzinfo=None, minimum_age=22, maximum_age=60)

Generate a random certificate (bs, ms, or phd) record['certificate'] = random.choice(['Bs', 'Ms', 'PhD'])

Select a random department

record['department'] = random.choice(list(dept_jobs))

Select a random title that associative with each selected department record['title'] = random.choice(dept_jobs[record['department']]) Generate a random level

record['level'] = random.randint (8,1)

The method to calculation salary was done by using following steps: Calculate salary based on age, level, and certificate

```
age = 2023 - birth_year
min_salary, max_salary = level_salaries[record['level']]
certificate_multiplier = {'Bs': .45, 'Ms': .75, 'PhD': 1}
salary = round (random. uniform (min_salary, max_salary) * (age / 22) *
certificate_multiplier[record['certificate']])
 record['salary'] = max (min_salary, min(max_salary, salary))
```

all these features stored as comma-separated value (csv) file in order to use it in the methodology.

4.3 Unique Key Generate

Unique key generator, as-showing in Figure (4.2), has been calculated by lower key size, upper key size, digits, and punctuation. Generate random characters for each category without duplicates. Calculate the number of characters for each category based on percentages

```
lowercase_count = int (key_length * 0.25)
uppercase_count = int (key_length * 0.25)
digits_count = int (key_length * 0.125)
punctuation_count = int (key_length * 0.375)
```

Combine all categories into a single list, shuffle the list to randomize the characters, and then convert the shuffled list back to a string and return it as the AES key

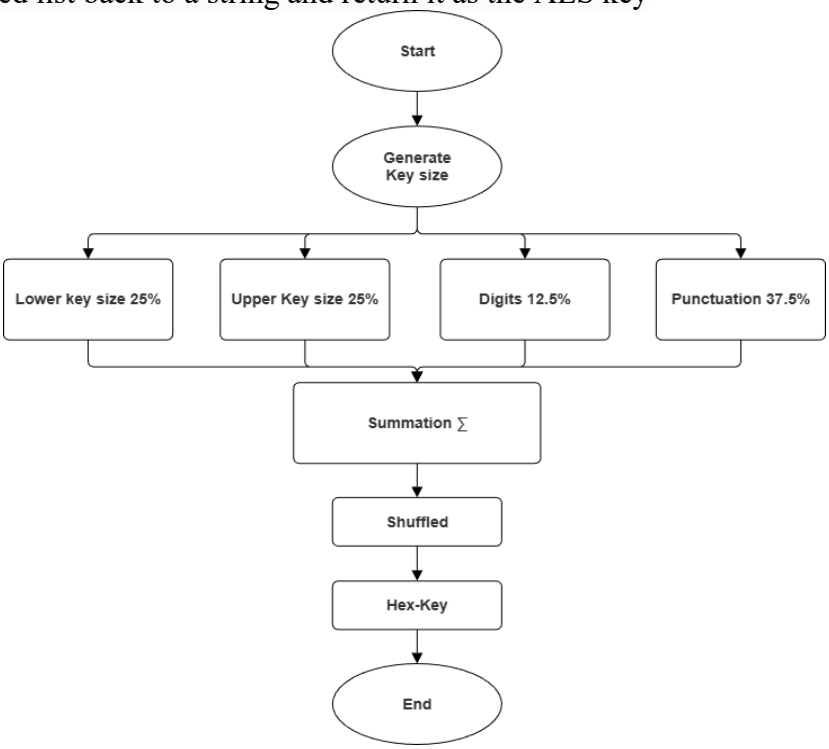


Figure (4.2) Shows the Structure of Unique Key Generator

The following-flowcharts describe the four steps of generate-unique key generator;

1) Lower Key size 25%,
2) Upper Key size 25%,
3) Digits 12.5 %,
4) Punctuation 37.5%

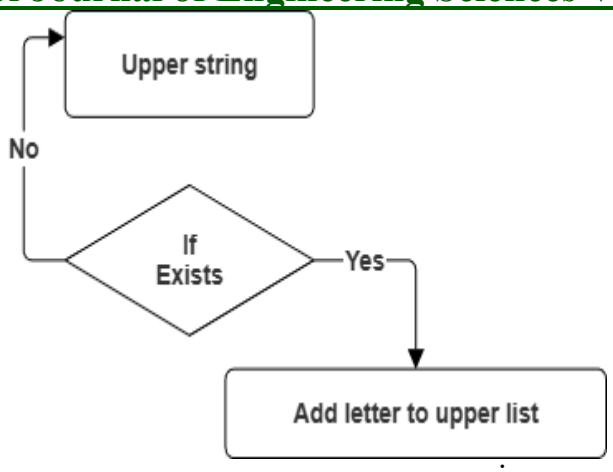


Figure (4.3) Shows the Lower Key Size 25%

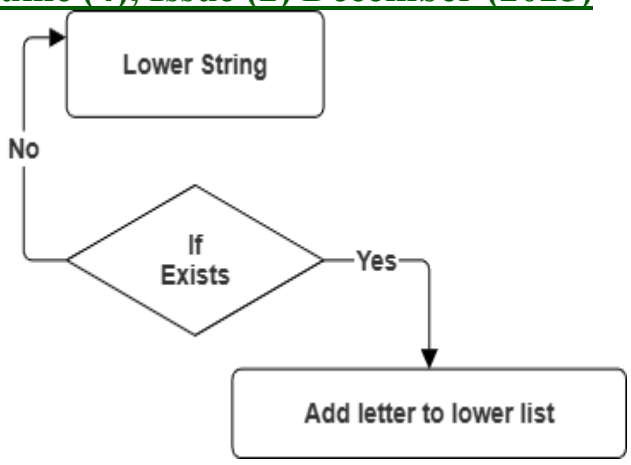


Figure (4.4) Shows the Upper Key Size 25%

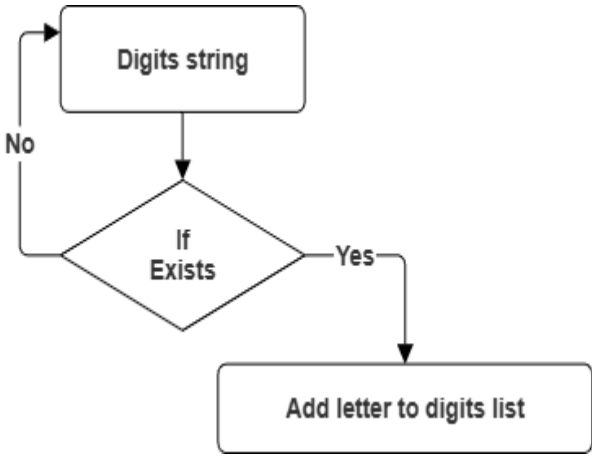


Figure (4.5) Shows the Digits 12.5 %

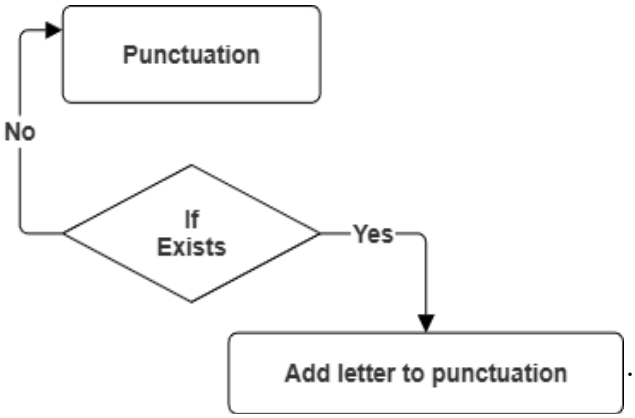
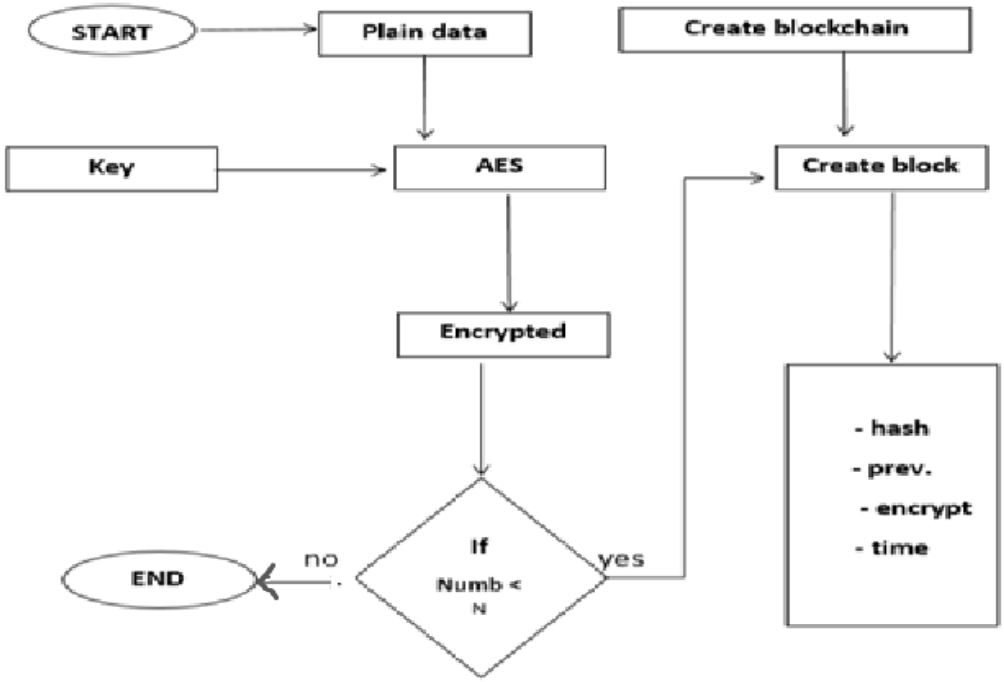


Figure (4.6) Shows the Punctuation 37.5%



The following-flowchart shows the encryption data of propose method

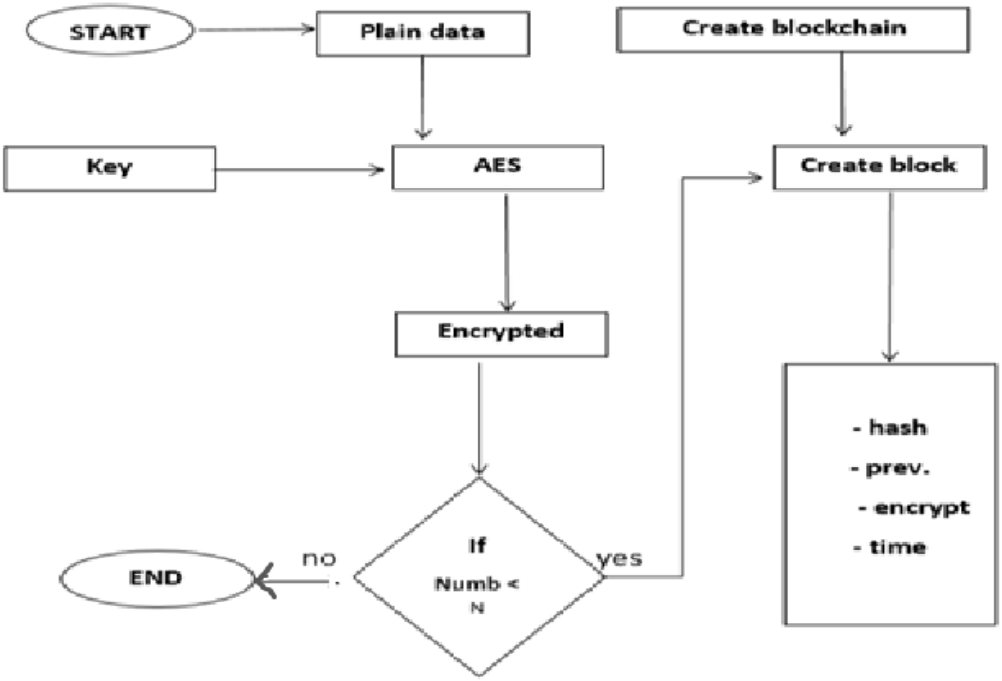


Figure (4.7) Shows the Encryption Data of Propose Method

Algorithm 3.1

Input: data set
dataSteps:
1- Load data.cvs
2- Generate unique key using hash function
3 - Generate key using size of each category
4- Key generate =lower 25%, upper 25%, digit 12.5% and punctuation 37.5%
5- ∑ key generates
6- Shuffled (key generate)
7- Encrypted data = hex key

4.3.1 AES Key Generator

The Advanced Encryption Standard (AES 256) is a highly secure symmetric encryption technique that employs a 256-bit key to transform plain text or data into a cipher, rendering it extremely difficult to decipher. The utilization of Base64 encoding systems is prevalent in scenarios where binary data requires encoding, particularly for storage and transmission purposes through text- oriented media. The utilization of encoding techniques serves the purpose of preserving the integrity of data during its transmission, hence preventing any alterations or modifications.

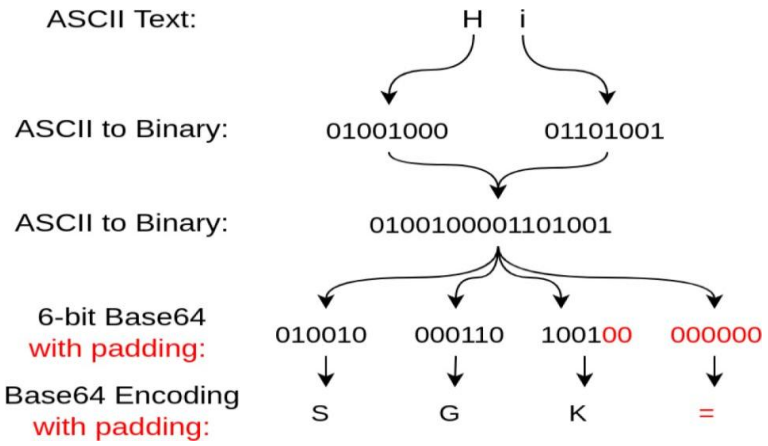


Figure (4.8) Shows the Base64 Encoding Process

4.3.2 Encryption Using Timestamp

Records the time taken for timestamps are commonly employed to encode data regarding the occurrence of specific events, typically encompassing both the date and time of day. In many cases, these timestamps are capable of providing an exceptionally precise measurement, even down to fractions of a second. The utilization of timestamps is not inherently linked to an absolute concept of time; they can be established with reference to any epoch and can be relative to any arbitrary point in time, such as the system's initiation time or a particular historical event. The inherent flexibility of timestamps enables their utilization across various contexts and systems, offering significant insights into the temporal sequencing of events, while avoiding limitations imposed by a universally

standardized time framework.

Figure (4.9) Shows the Calculation Timestamp for encrypted records

4.3.3 Created Blockchain Timestamp Using SHA-256 Algorithm

SHA-256 online tool helps to calculate hash from string or binary data, which can allow us to

encryption data in the blackchin. And the records of the time taken for blockchain has been creationas well as Blockchain with encryption data.

4.4 Plot Sample of Output Data

Perform the output of the algorithm 3.1 by plotting using random 4 blocks samples, the model proposed show that hash function, previous hash, encrypted data, timestamp, and block number changed randomly in each time of execution process. Figure (4.10) shows the blockchain information with blockchain sample.

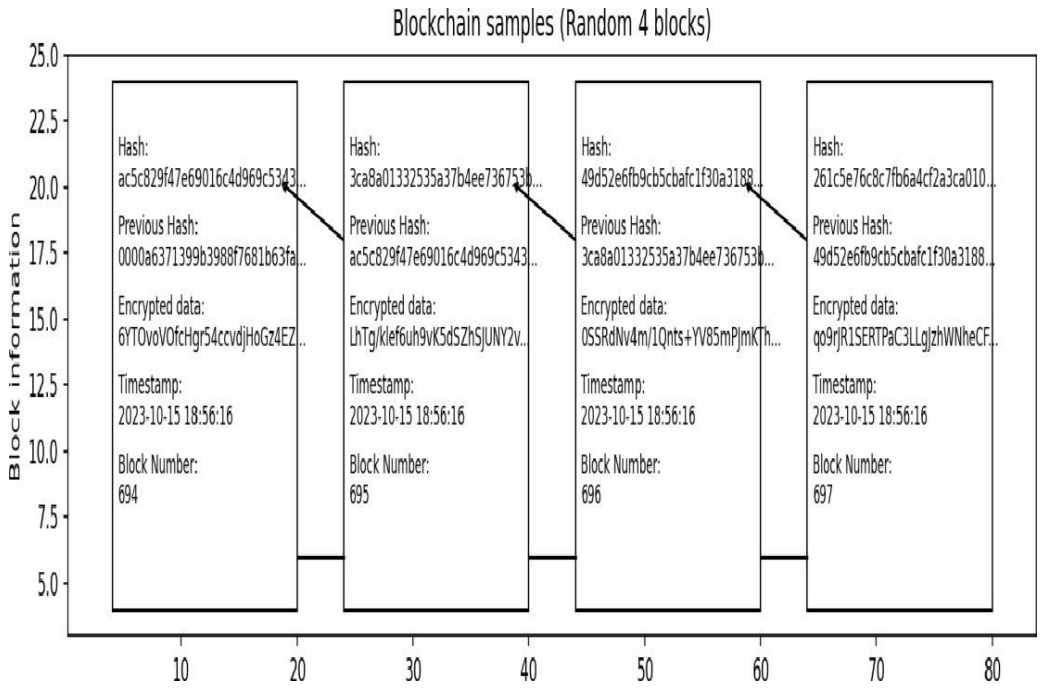


Figure (4.10) Shows the Output of Blockchain Sample for Algorithm 3.1

5. Results and Discussions

The model has been tested in the "national institute of standards and technology" (NIST). The results show that the model working perfectly, therefore show the model was successfully passed with 12 features and fall with 3 features, mean that 80%passed 20% fall, thus test has been done under key encryption test. Otherwise, model has been tested on cipher text, and the result show that the model was successfully passed with 11 features and fall with 4 features, the percentage of successfully was 74% and fall in 26%. Figures (5.1) and (5.2) shows the test of model.

5.1 Test Suite for NIST Number on Key Encryption:

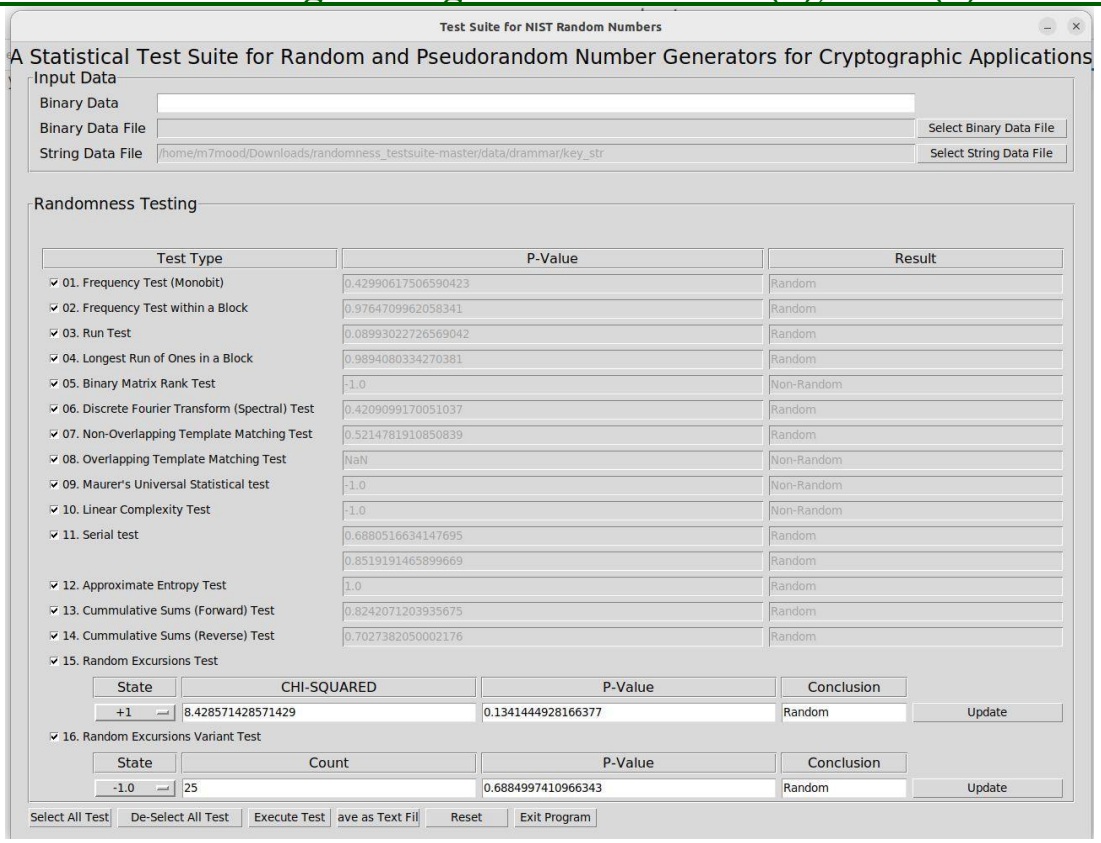


Figure (5.1) Shows the Result of NIST Test on Key Encryption

According to figure (5.1), test suite for NIST random numbers [19], show that model fall in four features ("binary matrix rank test", "overlapping templet matching test", "Maurer's universal statistical test", "and liner complexity test"), and successfully with other features.

5.2 Test Suite for NIST Number on Cipher Text

The conclusion demonstrates randomizing data test and the model tested with nine iterations in order to obtained the results. Figure also show the range of data tested with P-Value between (+1, -1). The state of "CHI-SQUARED" is 8.428. The provided description of the "Chi-squared" test is deemed to be accurate. The Chi-squared test is a statistical technique employed to assess the degree of association between observed data and expected data, with the aim of discerning whether the disparities between the two datasets are attributable to random variation or if they signify a meaningful relationship between the variables under investigation. The assessment of the independence of categorical variables and the testing of hypotheses regarding the distribution of categorical data are widely employed in diverse disciplines, including statistics, biology, and the social sciences. The Chi-squared test is employed by researchers to assess the presence of a statistically significant association between the variables being examined by comparing the observed frequencies with the expected frequencies. Test suite for NIST number on cipher text

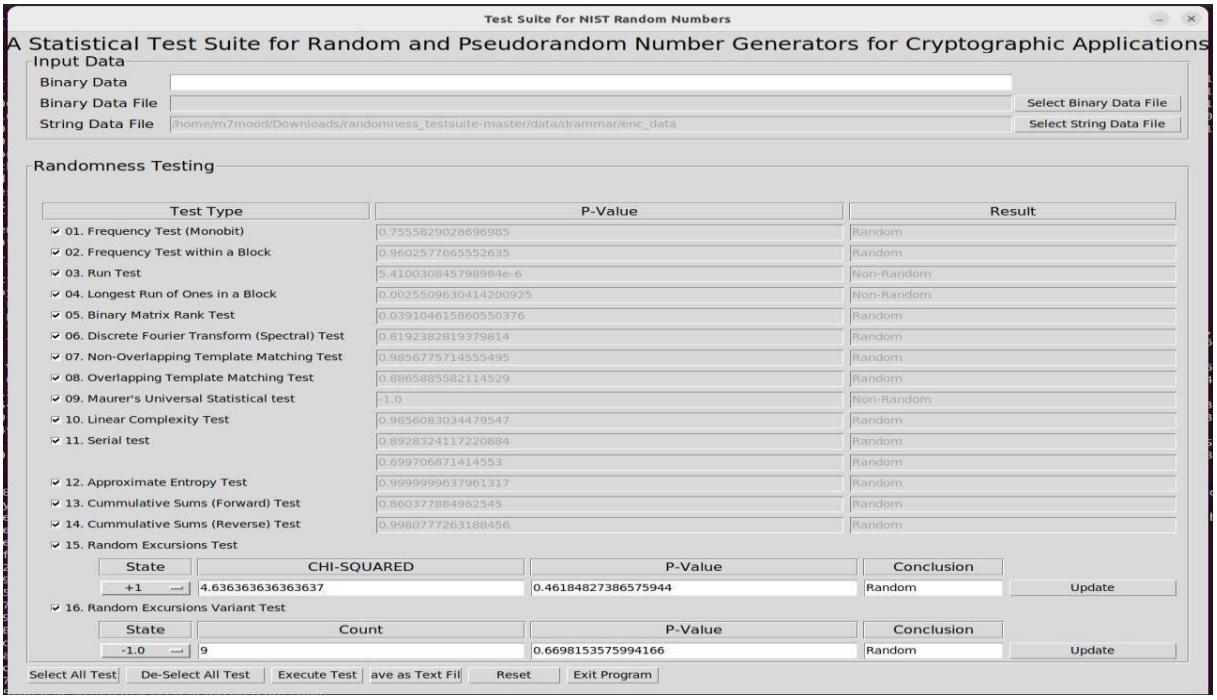


Figure (5.2) Shows the Result of NIST Test on Cipher Text

Figure (5.2), shows the test model on key encryption, the procedure of testing in the cipher textwas repeating on key encryption text in order to check the successfully model.

The test suite in NIST random numbers show that model fall in three features ("run test", "longest run ofœin clock", and "Maurer's universal statistical test"), and successfully with other features.
The description of "Chi-squared" test. The Chi-squared test compares observed data with expected data to determine if the differences are due to chance or a relationship between the variables being studied. It is used in statistics, biology, and social sciences to test hypotheses about categorical data distribution and variable independence. Researchers use the Chi-squared test to determine if variables are significantly related by comparing observed and expected frequencies.

6. Conclusions and Recommendations

6.1 Conclusions

This paper proposes a system that enables customers to easily grant or revoke record-specific authorizations to authorities through a simple tap. The deployment of this automation has been significantly facilitated by the utilization of Ethereum and smart contracts. The proposed wallet functions as an intermediary for facilitating secure and convenient entry to the blockchain. Additionally, the utilization of cryptographic encryption techniques, known for their formidable resistance to decryption, will ensure robust security and reliability. The successful implementation of blockchain technology has facilitated the authentication, data exchange, and security of HR payroll reports. Moreover, it can be inferred

1. Unique key was given a strong encryption, unique key has been using a key of features such as word, sample, numbers, and punctuation without repeating same feature of in the key.
2. Hash function with randomize hash in blockchain also gives strong encryption stage.
3. Model was testing on NIST and Entropy test, the result related with key was 80% randomize and 20% nonrandomized, while the result of testing in NIST in the string of cipher text was

76% randomize and 24% nonrandomized.

6.2 Future Works (Recommendations)

A blockchain, the utilization of a linked sequence of blocks for record maintenance has facilitated the development and implementation of novel programs that adhere to a distributed and decentralized ideology, as opposed to conventional cloud-based applications. In terms of future development, it is highly probable that the following objectives will be pursued: The present smart contract will be extended to improve the lookup and provide the advanced features required by an EHR administration system, for future works we recommended the following :

1. The utilization of AES-512 and RSA algorithms may be employed to enhance the level of complexity in the encryption process. The RSA technique, specifically RSA encryption, can be employed by utilizing the RSA key as an input key in AES-512 encryption, thereby offering a high level of encryption complexity.
2. The implementation of intelligent services in Blockchain, utilizing AES encryption, serves as an effective means of safeguarding services and preventing unauthorized access.
3. We recommended trying, if it is possible to uses of blockchain technology in context of electronic health records and the healthcare sector.

References

[1] Pinna, A., & Ibba, S. (2019). A blockchain-based decentralized system for proper handling of temporary employment contracts. In Intelligent Computing: Proceedings of the 2018 Computing Conference, Volume 2 (pp. 1231-1243). Springer International Publishing.

[2] Koncheva, V. A., Odintsov, S. V., & Khmelnitski, L. (2019). Blockchain in HR.In International Scientific and Practical Conference on Digital Economy (ISCDE 2019) (pp. 504-507). Atlantis Press.

[3] Wang, H., Qin, H., Zhao, M., Wei, X., Shen, H., & Susilo, W. (2020). Blockchain-based fair payment smart contract for public cloud storage auditing. Information Sciences, 519, 348- 362.

[4] Leng, J., Zhou, M., Zhao, J. L., Huang, Y., & Bian, Y. (2020). Blockchain security: A survey of techniques and research directions. IEEE Transactions on Services Computing, 15(4),2490-2510.

[5] Guo, L., Xie, H., & Li, Y. (2020). Data encryption based blockchain and privacy preserving mechanisms towards big data. Journal of Visual Communication and Image Representation, 70,102741.

[6] Kollu, P. K. (2021). Blockchain techniques for secure storage of data in cloud environment. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(11), 1515-1522.

[7] Ali Mir Arif Asif Ali.(2025). A Comprehensive Review on Artificial Intelligence & Blockchain Technology for Human Resource Management System. International Journal of Research and Analytical Reviews (IJRAR 2025), Volume 12, Issue 1.(pp.233-244) www.ijrar.org (E-ISSN 2348-1269, P- ISSN 2349-5138).

[8] Wasiu Eyinade, Onyinye Jacqueline Ezeilo, Ibidapo Abiodun Ogundeji. (2025). Blockchain Technology: Revolutionizing Transparency, Trust, and HR Processes in the Insurance Sector World Journal of Innovation and Modern Technology E-ISSN 2756-5491 P-ISSN 2682-5910, Vol 9. No. 6 2025,

pg320.328, www.iiardjournals.org online version DOI: 10.56201/wjimt.

[9] Farah Shaikh, Afroz Sial, Khalida Khan, Muhammad Naeem. (2025). FinTech-Enabled HR Payroll Automation and Its Effect on Employee Satisfaction and Brand Image. Advance Journal of Econometrics andFinanceVol-3, Issue-4, 2025, Online ISSN 2959-8990-Print ISSN-2959-8982,https://ajeaf.com/index.php/Journal/About.

[10] Minanda Putri Ramadhan, Tino Kemal Fattah, Putriana Salman. (2025). Optimization of Payroll Management through the Implementation of an Accounting System in the Public Sector. Journal of Business Transformation and Strategy, ISSN: 3047-2644, Volume 02 Issue 01, https://journalmab.ulm.ac.id/index.php/jbts

[11]Muhammad Khairi, Didit Darmawan. (2025), Blockchain Enforcement in Employee Data Management to Increase Transparency and Security. International Journal of Service Science, Management, Engineering, and Technology, Vol. 7 No. 2 (2025): https://ejournalisse.com/index.php/isse/article/view/132

[12]Xu, X., Sun, G., Luo, L., Cao, H., Yu, H., & Vasilakos, A. V. (2021). Latency performancemodeling and analysis for Hyperledger fabric blockchain network. Information Processing & Management, 58(1), 102436.

[13]D. L. Hernández-Rojas, T. M. Fernández-Caramés, P. Fraga-Lamas and C. J. Escudero, "Design and practical evaluation of a family of lightweight protocols for heterogeneous sensingthrough BLE beacons in IoT telemetry applications", Sensors, vol. 18, no. 1, pp. 57, Dec. 2017.

[14]T. M. Fernández-Caramés and P. Fraga-Lamas, "Towards the Internet of smart clothing: A review on IoT wearables and garments for creating intelligent connected e- textiles", Electronics, vol. 7, no. 12, pp. 405, 2018.

[15]Mochurad, L., & Shchur, G. (2021, March). Parallelization of Cryptographic Algorithm Based on Different Parallel Computing Technologies. In IT&AS (pp. 20-29).

[16]Ali, S., Javaid, N., Javeed, D., Ahmad, I., Ali, A., & Badamasi, U. M. (2020). A blockchain-based secure data storage and trading model for wireless sensor networks.In Advanced Information Networking and Applications: Proceedings of the 34th International Conference on Advanced Information Networking and Applications (AINA-2020) (pp. 499- 511). Springer International Publishing.

[17]Krumay, B., Bernroider, E. W., & Walser, R. (2018). Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering theNIST cybersecurity framework. In Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings 23 (pp. 369-384). Springer International Publishing.

[18]Azzahra, N. J. Implementasi Tanda Tangan Digital untuk Pengamananan Dokumen Digital pada Pelaksanaan Smart Governance.

[19]https://saviynt.com/glossary/national-institute-of-standards-technology-nist