International Journal of Electronics Engineering (ISSN: 0973-7383
Volume 11 • Issue 1 pp. 441-446 Jan 2019-June 2019 www.csjournals.com

Quantum Key Distribution Verifiable and Traceble Cipher Text Policy Attribute Based Encryption (QKD-VT-CPBE) Secured Model for Treasury Information System - E-Governance

[1]Prof. Ramineni Sivarama Prasad, [2]Gurram Veera Raghavaiah
[1]Research Guide, Department of Computer Science & Engineering, Acharya Nagarjuna University, Guntur, AP
[2]Research Scholar in Department of Computer Science, Raualaseema University, Kurnool, AP

Abstract: Security is one of the most important issues in E-governance projects. E-governance applications will be increasingly used by the citizens of many countries to access a set of government services. Currently, the use of the E-government applications arises many challenges; one of these challenges is the security issues. E-government applications security is a very important characteristic that should be taken into account. This paper analyses about new secured model developed for Treasury Information System by using Quantum Key Distribution based verifiable and traceable cipher text attributes based encryption (QKD-VTCP ABE) algorithm that support an integrated internet-based E-governance applications.
Keywords: E-governance, Security Model, QKD-VTCP ABE, SWOT Tool, NLT, Preprocessing, Key Generation, Encryption, Decryption.

1. INTRODUCTION.

The treasury information systems generally get defined by a unified structure for enabling the appropriate utilization of resource by the government banks. A treasury enables the bank in the transaction of the resources such as cash and payment receipts as these get linked with numerous other banking sectors. Thus, a consolidated view of the entire transactions is observed by the government organization through the treasury system at any given time. Furthermore, the appropriate implementation of the treasury system was found to eliminate the accounting situations observed among several public organizations regarding revenues, incomes and receipts. Moreover, a TIS is a significant factor in reforming the government sectors to manage the resources efficiently considering sustainability. Thus, the process involved in the collections, payments, transparency and accountability of resources were found to get improvised while considering the treasury systems (Dandago and Rufai, 2014).

The emerging advances in information technology were observed to get utilized in diverse applications such as factories, communications, entertainment, banking, transportations, educations, etc. This technology was found to optimize the resources such that an intelligent decision-making process got implemented for accelerating economic growth, improvise the governance and for efficient development of the resources (Anderson et al., 2015). The emergence of e-governance got initiated for the automation of government objectives, for enabling the access of web functions to the citizens and for improvising the effectiveness and efficiency of the involved process(Kumar,2015)

An increase in the dependence of the computerized system for the investment purposes by numerous organizations in diverse applications got noticed in the recent scenarios — the emergence of this technology as found to create a variance in the methodology regarding auditing. However, the proliferation of this technology was observed to develop numerous issues concerning data integrity, abuse, privacy issues etc. Therefore, while an IT system was found to have got implemented in a surrounding that is deficient of hardware, and controls in comparisons to the existing manual systems. Thus, while considering the information system, it is necessary to consider an independent audit for developing adequate measures in the design and operations concerning the various risks involved in the system (Linders, 2012). Besides, Treasury Information System was found to get incorporated with diverse parameters such as financial audits, operational audits, specialized audit and forensic audits. These factors were concerned with approaches employed for accessing the financial statements of organizations, for evaluating the control structures internally, auditing involved in the performance and in assessing the third party for the outsourcing of the resources. Furthermore, the significant functions of the and the treasury systems were found to include the assessment and evaluation for ensuring the safety of the process.

This process was found to get incorporated with diverse assets such as data, technology, application facilities and individuals.

Therefore, considering the present scenario applications of the treasury information systems, it is necessary to develop an efficient model comprising of attributes such as information, effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability of information.

2. PROBLEM STATEMENT

The Indian government adopted a Network and Information security measures as a part of e-Governance to protect the vital information's that got incorporated in the framework involving the e-Governance. The major challenges observed in the design of the e-governance system was found to be regarding risk involving the security of the data shared among the network. Therefore, it is necessary to address the issues regarding the security issues that are incorporated within an E-governance project as it comprises of critical information's that get transmitted through Intranet and LAN. Thus, for maintaining the confidential data, it is necessary to develop an appropriate model based on the treasury information system. The security is critical was found to be some significant challenges in the e-Governance to safeguard the assets and maintain the confidentiality of transactions and information on the network. Government documents such as online funds transfer, birth and death registration, vehicle license, passport applications, land documents etc. need to be protected from unauthorized users in e-Governance projects while incorporating the information systems. Hence security was found to be a critical aspect for the implementation of Treasury Information Systems on an integrated internet-based application. Furthermore, the majority of E-governance applications observed in India were found to be related to the applications on their Intranet. Thus, it is necessary to develop an appropriate integrated model devised in the form of an Integrated Internet-based system for providing the required in the by providing new security models on data and network transmission.

3.. AIM:

The research aims at designing a security system for protection of Treasury Information System.

4. OBJECTIVES:

The research has the following objectives to achieve the aim as mentioned above:
1. To explore the various existing Treasury Information Systems (TIS) and its challenges of various governments
2. To find the better functioning of Treasury Information Systems across the worldwide
3. To develop a CP-ABE based security algorithm for obtaining security to the Treasury Information System.
4. To evaluate the performance of a new proposed secured Treasury Information System model and to compare it with existing techniques.

5. PROPOSED METHODOLOGY :

Security is an important challenge in the Treasury Information System (TIS) model in-transmit over Local Area Network (LAN) and intranet. Also, government documents such as online funds transfer, birth and death registration, vehicle license, passport applications, land documents, etc. These documents have to protect from unauthorized users in e-Governance projects. Thus, security is the most critical issues in thee-Governance to safeguard the assets and maintain the confidentiality of transactions and information on the network. Therefore, the solution is that to develop a new high-security algorithm for Treasury Information Systems on an integrated internet-based application.

STEP 1: Obtain the information from the treasuries like workflow-based treasury payment/receipt transaction-processing system and perform the SWOT analysis.
Strength: Often, an organization's strengths provide an easy opportunity for increasing their security, by building on or positively modifying existing controls, security can usually get increased.
Weakness: Weakness can be specific or broad. A general lack of security program or culture is considered as the weakness but is not defined enough to guide action. Outlook on specific areas is necessary. Organizations fall prey to vulnerabilities that would not have got prevented if they had a proper patch management program.

Implementing a patch management program involves spending money, but it is a small price compared to remediating damage caused by an exploited vulnerability.
Opportunities: Opportunities are low hanging fruit over which you can take advantage. The best part is that taking advantage of most opportunities do not require management approval or any significant spending.
Threats:
Many threats, especially from a security perspective, are easy to delineate. If the organization is subject regulations such as PCI DSS, HIPAA or SOX, the cost of non-compliance can be astronomical. The costs of reputational damage often outweigh the fines for non-compliance. And the fines for non-compliance are stiff.

A SWOT analysis is an essential test for implementing any plan. For acceptance of the plan, strength and opportunities should outweigh the weakness in the plan and possible threats that may arise on applying it.

STEP 2: From that data, need to pre-process the text using natural language machine learning to get effective information.
Preprocessing consists of four parts, they are Cleaning, Annotation, Normalization and Analysis
Cleaning:
It consists of getting rid of less useful parts of the text through stop word removal, dealing with capitalization and characters and other details.
Annotation:
It consists of the application of a scheme to texts. Annotations may include structural markup and part-of-speech tagging.
Normalization:
It consists of the translation (mapping) of terms in the scheme or linguistic reductions through Stemming, Lemmatization and other forms of **standardization.**
Analysis:
It consists of statistically probing, manipulating and generalizing from the dataset for feature analysis.

STEP 3: Once the pre-processing is done, by developing a conceptual framework using Quantum Key Distribution based verifiable and traceable cipher text attributes based encryption (QKD-VTCP ABE) algorithm.

Quantum Key Distribution (QKD)

With the exponential growth of network bandwidth, computational resources and the popularity of the internet, cloud security has become one of the interesting research areas of cloud computing.
Cloud computing services are used widely in different applications such as medical, defense, education, health etc., for data storage and elastic computing. Attribute-based encryption is a public key encryption algorithm that allows cloud users to secure their sensitive information in the public cloud servers. Traditional attribute-based encryption models apply to standalone applications with limited resources constraints, in-secured key generation and slower processing speed. Also, users‟ data access control mechanisms must satisfy the process of protecting data from unauthorized users as well as from third-party providers. To overcome these issues a novel quantum key distribution (QKD) based cipher text-policy ABE model got implemented in the cloud environment.

Verifiable and Traceable Cipher-Attributes Based Encryption scheme (VTCP-ABE) simultaneously supports the properties of verifiable outsourced decryption and white-box traceability without compromising the physician's identity privacy.

STEP 4: When the QKD-VTCP ABE applied it first takes the text data and encode the information and key will get generated.

The scheme is for ciphering and deciphering the information for a secured transfer. Quantum Key distribution gets applied to verifiable and traceable Cipher which encrypts based on attributes. The information is encoded, and the key for decryption gets sent along with the encoded information. The generation of the key gets after encoding the data, and this key decrypts at the destination node.

STEP 5: Key gets sent to the cipher text, from that the text data will be decoded and generate key secret.

International Journal of Electronics Engineering (ISSN: 0973-7383
Volume 11 • Issue 1 pp. 441-446 Jan 2019-June 2019 www.csjournals.com

Cipher text receives the key, and the text data gets decoded and requires the key secret that gets used for decoding for analysis.

STEP 6: Once the decoding gets done, then from that generated key data we get exact text and compare efficiency with the existing algorithm.

After decoding the secret information, the text received gets compared with the original text. The comparison will show the efficiency of the existing algorithm.

Given below is the flow chart for the proposed security system in Treasury Information System

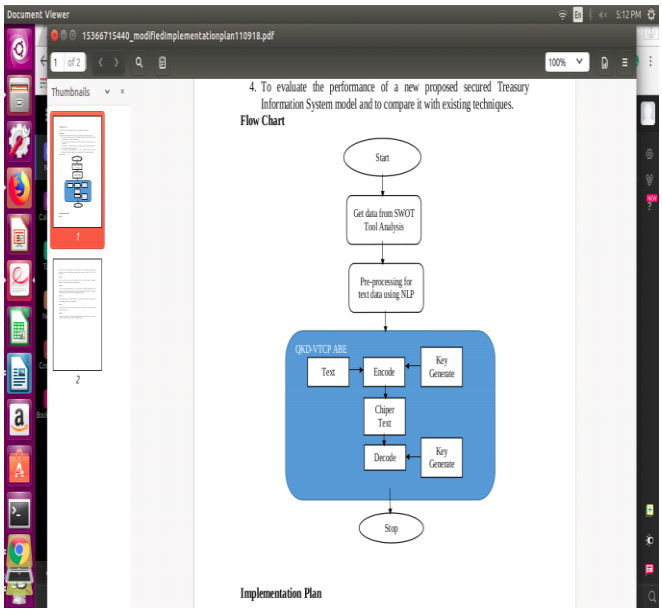
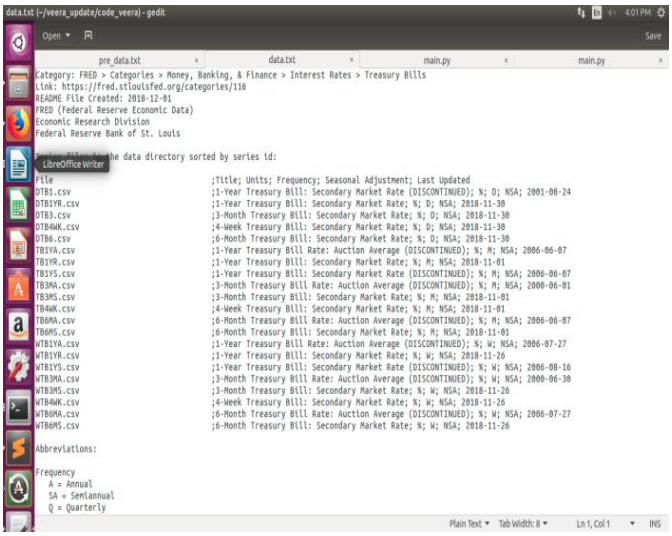


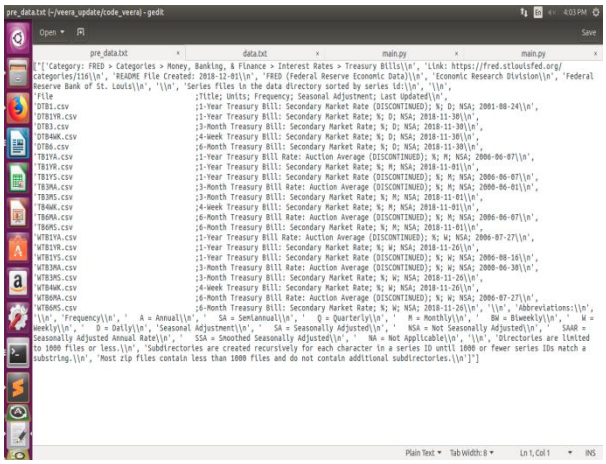
Fig.1: PROPOSED SYSTEM

Implementation Procedure:
Step 1:
Collecting datasets from indian treasury website in internet. After collecting data we need to do preprocessing.
Step 2:
Data we need to store .txt document, after that we can read data using reading command in python programming.

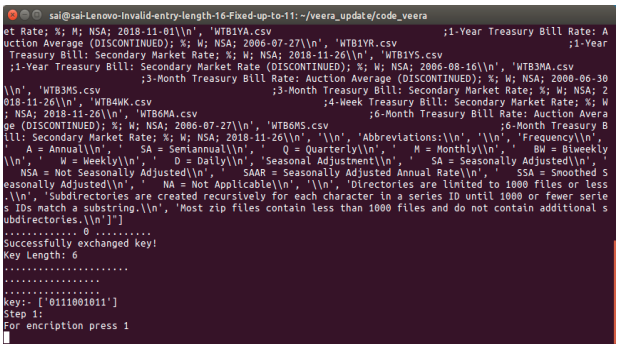


International Journal of Electronics Engineering (ISSN: 0973-7383
Volume 11 • Issue 1 pp. 441-446 Jan 2019-June 2019 www.csjournals.com

Step 3:
Initial data having any special characters are any unwanted data are punctuations we need remove and arrange as proper text using natural language process. In python programming this is the advanced feature for text preprocessing. Using NLTK we can remove unwanted data and arranging as a proper manner.



Step 4:
After preprocessing, we need to give preprocessing data to QKD based cipher text attribute based encryption. In QKD(quantum key distribution) we can generate public key for encrypt and decrypt data. Quantum key Distribution is a protected specialized strategy which executes a cryptographic convention including segments of quantum mechanics. It empowers two gatherings to deliver a common irregular mystery key known just to them, which would then be able to be utilized to scramble and decrypt messages.
An important and unique property of quantum key distribution is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This results from a fundamental aspect of quantum mechanics: the process of measuring a quantum system in general disturbs the system. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superposition or quantum entanglement and transmitting information in quantum states, a communication system can be implemented that detects eavesdropping. If the level of eavesdropping is below a certain threshold, a key can be produced that is guaranteed to be secure, otherwise no secure key is possible and communication is terminate.



BB84 is a QKD scheme. It is the first quantum cryptography protocol.The protocol is provably secure, relying on the quantum property that information gain is only possible at the expense of disturbing the signal if the two states one is trying to distinguish are not orthogonal and an authenticated public classical channel. It is usually explained as a method of securely communicating a private key from one party to another party for use to encryption.

Step 5:
After generating private key using QKD, then we can save the private key and apply ciphertext policy based encryption technique to encrypt the data. CPABE we have different schemes of encryption techniques to encrypt the data, here we are using advanced encryption technique to securely transfer from alice to bob. and supports a block length of 128 bits and key lengths of 128, 192, and **256** bits.

Step 6:
In our code it will ask press 1 for encryption, after we need to give preprocessing filename to encrypt the data. Encrypted data was converted to cipher text and it will stores filename of encrypted_preprocessing.txt.

Step 7:
In the same process we need to do while running decryption side also, For decrypting the data we need to run decry.py. After running it will ask to press 2 for decryption. It will ask again encrypted file to decrypt the cipher text, after giving the encrypted file it will ask key, In QKD we have generated private key that same key we need to give same decryption side, it will decrypt the file. We will get data same like original data.

SIGNIFICANCE OF STUDY

The proposed research is hypothesized to improve the overall cyber security of the governance by reducing the cost and improvising the effectiveness of the government machinery. Thus, the research will enable the development of an efficient, accountable and transparent functioning system for diverse applications.

REFERENCES

- Dandago, K. I., &Rufai, A. S. (2014). Information technology and accounting information system in the Nigerian banking industry. Asian Economic and Financial Review, 4(5), 655-670.
- Linders, D. (2012). From e-government to we-government: Defining a typology for citizen coproduction in the age of social media. Government Information Quarterly, 29(4), 446-454.
- Anderson, D., Wu, R., Cho, J. S., & Schroeder, K. (2015). Introduction: Global Challenges in Turbulent Times: Road to Sustainable E-government. In E-Government Strategy, ICT and Innovation for Citizen Engagement (pp. 1-10). Springer New York.
- Kumar, T. V. (2015). E-governance for smart cities. In E-governance for Smart Cities (pp. 1-43). Springer Singapore.
- Dandago, K. I., &Rufai, A. S. (2014). Information technology and accounting information system in the Nigerian banking industry. Asian Economic and Financial Review, 4(5), 655-670.
- Tootoonchian, et al. (2008): Locker: social access control for web 2.0. In: WOSN
- Luo, W., Xie, Q., Hengartner, U(2009).: Facecloak: an architecture for user privacy on social networking sites. In: International Conference on Computational Science and Engineering, CSE 2009, vol3. IEEE
- Sahai, A., Waters, B. (2005): Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg
- Rouselakis, Y., Waters, B. (2013): Practical constructions and new proof methods for large universe attribute-based encryption. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM
- Pirretti, M., et al. (2006): Secure attribute-based systems. In: Proceedings of the 13th ACM Conference on Computer and Communications Security. ACM
- Baden, R., et al. (2009): Persona: an online social network with user-defined privacy. In: ACM SIGCOMM Computer Communication Review, vol. 39., no. 4. ACM
- Yeung, C.M.A., et al. (2009) Decentralization: the future of online social networking. In: W3C Workshop on the Future of Social Networking Position Papers, vol. 2
- Nilizadeh, S., et al. (2012): Cachet: a decentralised architecture for privacy-preserving social networking with caching. In: Proceedings of the 8th International Conference on Emerging Networking Experiments and Technologies. ACM
- B.N.V. Madhu Babu & Dr K. Rajasekhara Rao. (2017) A NOVEL QUANTUM KEY DISTRIBUTION BASED CIPHERTEXT POLICY ATTRIBUTE-BASED ENCRYPTION MODEL FOR CLOUD SECURITY. International Journal of Modern Trends in Engineering and Research.
- E Governance A Comprehensive Framework by D N Gupta, **SBN**: 8177081695, **Edition**:First, **Year Of Publication**: 2008.
- E Governance, **Author(s)** : Pankaj Sharma, **ISBN**: 8176485160 **Edition**:**Year Of Publication**: 2012.