

Notarial Office Certificate Generation, Authentication and Storage for user Requested Application based on Blockchain

Poornima D.
Student, CSE, M.Tech
Bangalore Institute of technology
Bangalore, Karnataka, India

Prof. Mamatha V
Assistant Professor, CSE, M.Tech
Bangalore Institute of technology
Bangalore, Karnataka, India

Abstract:- In the present recent studies have given that Blockchain is been more helpful in the well being of counties technology mainly with respect the e-Government updation in technology like e-voting, smart city concept and many more. Just like that the notarial office certificate issuing is the part of e-government which place an important role in ones life. So, this could be done easy with the Blockchain Technology (BT). We propose an AES Encryption and decryption method of file storing and mongo DB which is used for the status and information of the application submitted will be stored. In the existing System of the notarial office is old method in which the user as to hardcopy of the application for required certificate and all the validation, collecting the certificate all done manually. But this work make it easy for both user and officer, Where the user would get the certificate from the officer by the grid API method of email which provides the password for the certificate download.

Keywords:- Blochchain Technology(BT), Notarial office, Certificate, e-Government, AES Encryption and decryption.

I. INTRODUCTION

The Notarial Office (NO), which is attempting to provide various necessary certifications, still relies on human labour and needs paper supplies from other government agencies. There are many other inconveniences as a result. One of the notary's primary responsibilities is to verify a person's signature. Blockchain may indeed be used to improve the process and make it more convenient and easy. For automating Notary Of services, a blockchain-based solution is appropriate. In order to enhance performance, a project might also suggest a better blockchain network structure. To satisfy the needs of the Notarial Office, a distributed system built on blockchain will be used. A series of tests will be run to assess the effectiveness and viability of this system. In addition, we establish additional ledgers to off-load various sorts of transactions, replace manual tasks with smart contracts, and offer encryption for sensitive data.

This project has a number of difficulties that have been recognised. The main goals of this study are to assess the difficulties in implementing Blockchain technology for certificate issuance, management, and verification. The notarial offices' certificates currently need to be handled manually. It seems more appropriate to build NO services using such technologies given the depth of development of

information and communication technology. The traditional e-system, on the other hand, is typically constructed on centralised infrastructure, which is weak and extensively regulated by outside parties. This makes it vulnerable to a single point of failure and means that system users can simply change the data that is stored there. Due to numerous inter-agency contacts, human error, and other factors, creating an e-service system based on centralised infrastructure can be advantageous.

The main objective of the system is to replace the manual process certificate issuing with the technology method. As any kind of government certificates place an important very important role in everyone life it helps in making the process easy . This system helps in getting the certificates more efficiently less time consuming.

In the e-Government the certificates of the notraial office place an important role like marriage certificate, birth certificate so as now also it is done with old method of collecting application filling as then make it validated finally after all the process the then the certificate with will be issued to the citizens.

There are several problems that have been identified in this project. The core objectives of this study are to evaluate the challenges of adopting Blockchain technology for issuing, managing and verifying certificate. The notarial office' certificates currently need to be handled manually. It seems more suitable to build NO services using such technologies given the depth of development of information and communication technology. The traditional e-system, on the other hand, is typically constructed on centralised infrastructure, which is weak and extensively regulated by outside parties. This makes it vulnerable to a single point of failure and means that system users can simply change the data that is stored there. Additionally, creating an e-service system based on centralized system might be beneficial since it can address issues with many inter-agency contacts, human labour requirements, and distances between various places.

II. RELATED WORK

In Governments now have new chances to fulfil strategic goals including citizen contentment and happiness, service efficiency, and cost optimization because to the e-ability government to record transactions on distributed ledgers. The network where it can also be validated and verified. "Consensus" refers to the process of creating a block and certifying it. The coalition In the corporate world, blockchain technologies are typically used to track cross-organizational business transactions[2]. a particular decentralised culture of information exchange built on mutual confidence amongst the stakeholders as a result of a computer protocol. It is comparable to a book that is accessible to everyone and located in a public area where anybody can openly register the action (trade, contract, etc.)[3].

The methods for requesting a certificate[1]. People obtain the Notarial's requisite application from several local government entities. The Notarial office will receive those hard copies. The Notarial office reviews each application individually before accepting or rejecting it. In the event that all documents are approved, the notarial office issues a specific certificate.

The Corruption in government for notarial certificate is the main threat where the By using the Panel Threshold Regression (PTR) and Feasible Generalized Least Squares (FGLS) models, respectively, researchers have determined the linear effect and threshold effect of e-government on corruption[4]. a Becker procedural model that supports the proposed model's architecture. Through two primary phases: Generation and Transfer, this technique explains how Maturity Models are generated, reviewed, and motivated. [5]. PRISMA is used to make sure that it is founded on repeatable and transparent procedures that enable the identification of all studies that satisfy the eligibility requirements and a methodical presentation of the findings[6].

The SOA in the public sector uses the E-Government based on cloud computing and service-oriented approach: a mix service made of services offered by both corporate and governmental units. Services are implemented using three technologies: REST technology, software component technology, and web service technology[7]. the administration of e-government information assets. then they create a collection of deep learning models with the intention of automating a variety of e-government functions. Finally, they put forth a smart e-government platform architecture that facilitates the creation and deployment of AI e-government applications[8].

In a social network, a blockchain-based transaction architecture for e-government requests is used. This framework provides an incentive mechanism to incentivize community members to spread the resources through a smart contract [9]. It focuses on how to provide a secure and convenient manner to exchange digital resources with the consent of the community. Multi-group analysis is used to assess the existing work scenario and how citizens' attributes

can influence how satisfied they are with required e-government services[10].

The conversion of an e-government data distribution service into a b-government equivalent is technically possible taking into account specific hardware and network requirements thanks to the permissioned blockchain platform known as Hyperledger Fabric, which is on a modularized environment capable of simulating real network conditions and architectures depending on the needs [11].

The developed model includes the identification that must be evaluated in order to establish the suitability of cloud computing to deliver e-government services in state sector institutions. IPMA has been carried out to rank management-oriented measures. And according to findings, cloud computing's relative advantage is particularly relevant to assessing its suitability for e-government implementation tasks due to its large impact[12].

LADM is a fundamental model made up of rights, limits, and responsibilities (RRR) and geometric elements that generates communication across templates. Whereas in this case, the method employed to establish a conceptual link between LADM and UML was UML[13]. Demand Analysis and Virtual Database Module Division Model using construction and K-means clustering The public can receive more convenient and effective government services thanks to a new Internet model based on metadata[14].

Citizens are informed about the pervasive e-services by social science and economics study for smart cities. the effects of modern infrastructure and technology-based service advancements on people's lives in contemporary societies[15]. Blockchain is used for digitization, and the KSI technology is utilised for greater volume of information and produces smaller unique hash values. It also only allows the authorised admin to monitor database changes[16].

In the covid pandemic the business of Polish property value was the first to be conducted in this specialized, normal narrow professional group which as affected, analysis by answering the questions posed out to what extent the professional activities of values were affected by COVID-19[17]. demonstrating WebVRGIS with the support of a convincing 3D model of Shenzhen. 3D visualization, also Geographic statistical analysis and integrating all types of key information [18].

The benefits and drawbacks of applying blockchain technology to public administration. demonstrates how both public and commercial organisations are using modern management technologies. Utilizing the PRISMA method[19] and the databases Scopus, Web of Science, SSRN, and Science Direct, researchers have found publications. information about transactions and digital assets in a peer-to-peer network. The data is secured, stored, and distributed via blockchain in a cutting-edge manner. The Google Scholar database's selection of 814 papers is analysed to locate relevant publications[20]. To increase efficiency, efficacy, cost-effectiveness, and openness, numerous governments throughout the world are launching

digital transformation efforts. Since most current e-government systems are standalone, establishing collaborative procedures is necessary for their integration and interoperability. Since e-government technologies are commonly accomplished in isolation, their integration and interoperability

III. METHODOLOGY

A. Overview

The existing system uses a normal offline mode the methods for requesting a certificate[1]. People obtain the Notarial's requisite application from several local government entities. The Notarial office will receive those hard copies. The Notarial office reviews each application individually before accepting or rejecting it. In the event that all documents are accepted, the notarial office issues a specific certificate. The primary issues with the current system include manual intervention, which takes more time and results in a high rate of data loss.

a) Notarail office:

A notarail officer is a person who has the authority to handle legal matters, especially witnessing signatures on papers. The notarial profession takes on several forms depending on the local legal systems. Despite being a member of the legal profession, a notary differs from an advocate in that they do not represent the client or take sides in come in many different shapes. Notarizing documents helps to prevent fraud and ensures that they were correctly executed. An unbiased observer (the notary) recognises signers to weed out impostors and ensure that they have freely and voluntarily engaged into agreements. Identifying the individual presenting before the notary by a personal connection or by reference to important documents such as a marriage certificate or birth certificate, among others, is also possible. Signatures can also be checked, recorded, and compared. Recording given with the certificate. Moreover, Certificates are not just a piece of paper; these documents are proof having specific details, it may be a skill, birth certificate etc. Typically, the certificates are produced on paper and that has some drawbacks. Paper certificates provided from NO need to be manually issued and verified; this process can be time-consuming. Unfortunately, there is a real problem with counterfeit paper certificates which can be made/purchased. The increasing problems affect the credibility of certificates as well.

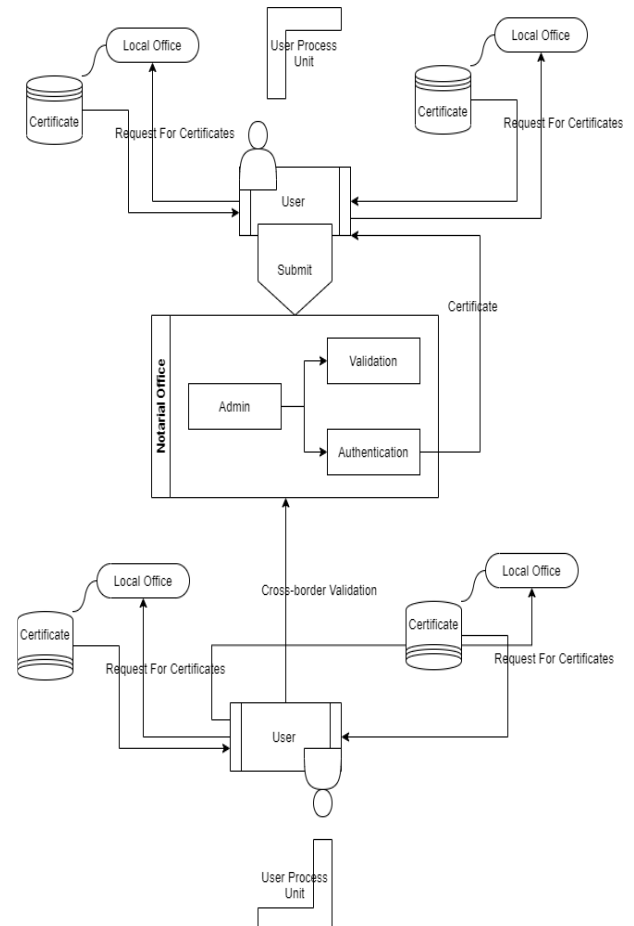


Fig. 1: Existing system for requesting certificate

b) Blockchain and MongoDB :

Blockchain provides very well advancement for more solutions for managing public information that are decentralised. Blockchain technology in e-government could automate public information operations. The systems for e-healthcare, e-migration, e-cities, and e-armies can all be automated. The more hashing valued algorithm makes the data to be authenticated and protected safely.

The other hand Mongo DB which is With its strong, unified query API and document data format, which corresponds to how programmers think and write code, MongoDB enables quicker, more flexible application development.. In our work the status of the process and the information of the application submitted will be saved. The combination of the both the technology is been used for the process of requesting and generating the certificate.

B. AES Encryption and Decryption

In Blockchain Technology there are number of algorithms to be applied for the securing of the data. AES is an iterative cypher as opposed to a Feistel one. It is built on a network of substitution-permutations. It consists of a number of interconnected operations, some of which replace inputs with particular outputs and others of which entail moving bits about.

AES Encryption method is limited to describing an average AES encryption round. There are four sub-processes in each round. The first round procedure is illustrated here, and downloading the certificate is done using the bit key value that was obtained. The reverse order of the encryption and decryption steps in an AES are similar.

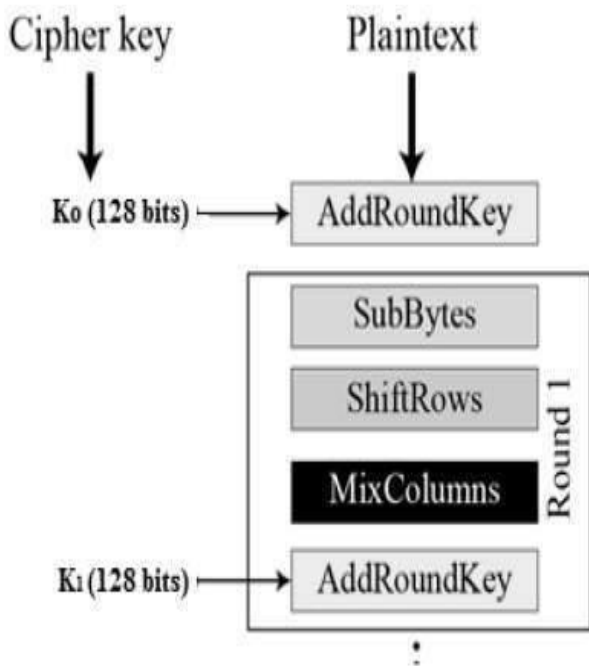


Fig. 2: AES Encryption and Decryption

C. Proposed system

In proposed To satisfy the needs of the Notarial Office, a decentralised blockchain-based application will be implemented. A number of experiments will be run to assess the system's effectiveness and viability. Additionally, we set up other ledgers to off-load various sorts of transactions, replace manual activities with smart contracts, and offer encryption for sensitive data as necessary. With the use of blockchain and smart contract technology, all stakeholders are handled.

The system has different stakeholders:

- Certificate Issuers/Committee Head The role of Certificate Issuer (NO) is to select the required template of certificate as per the submission and add the details of every individually or by bulk upload.
- Higher Authorities The Higher Authorities need to verify the pending certificates that have been issued by the Committee Head (NO)
- User The user receive the link of the certificate and then can download the soft copy of the certificate and can use this link or the e-copy for sharing the certificates.

- Administration The administrator could add, manage, delete all the Certificate Issuers, Higher Authorities etc.

As shown in the diagram below the user will login to the portal the application is uploaded to the portal. By the blockchain AES encryption the file is encrypted and saved in the blockchain where the smart contract places an important role. The other side the officer logs in with username and password and downloads the application uploaded by the AES decryption and verify the information in the application.

The verified application details will be stored in the mongo DB, the other officer will login and for validated application he changes the statues of the approval.

Then the API grid is used to send the email to the user by sharing the password where with the help of that password user can download the certificate.

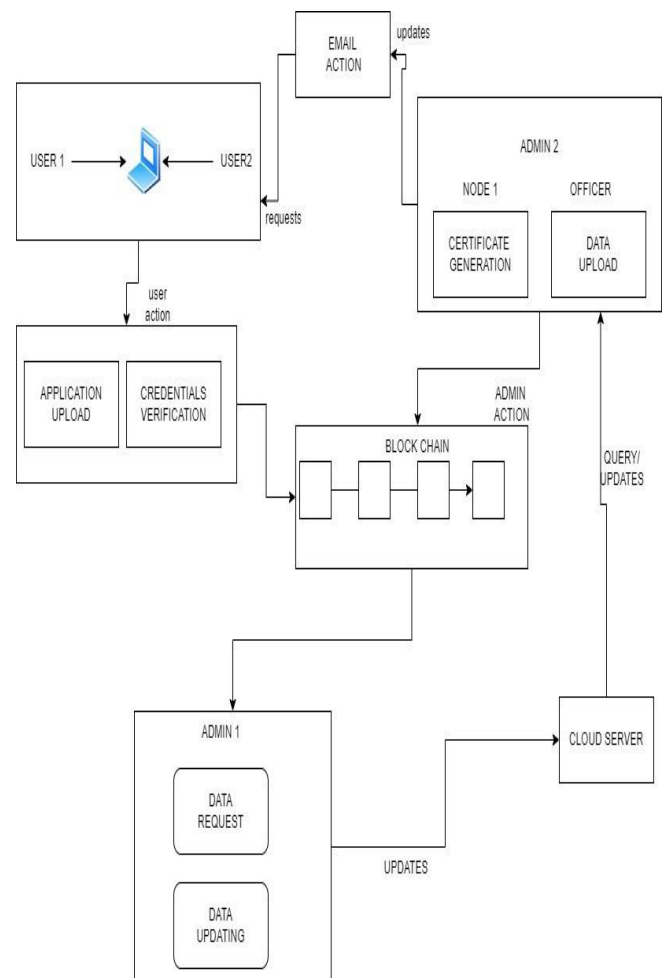


Fig. 3: Certificate generation model

The main application of the proposed system To address the issues with cross-border government services, an electronic certificates sharing system based on consortium blockchain has been developed. increase storage space efficiency and transaction storage. decreases the manual labour.

IV. RESULTS

The project provides graphic user interface in the form of web pages. The web pages are developed using Java Server Pages and html. The user interactive interface is developed for admin and notarial officer. The admin interface provides login page for credentials, home page with functions as buttons to choose the actions. The user interface provides a login page. The Figure 4 contains the login for both the user and the officer as shown in the above diagram. Figure 5: user side portal for application upload and download.



Fig. 4: Notarial office application portal

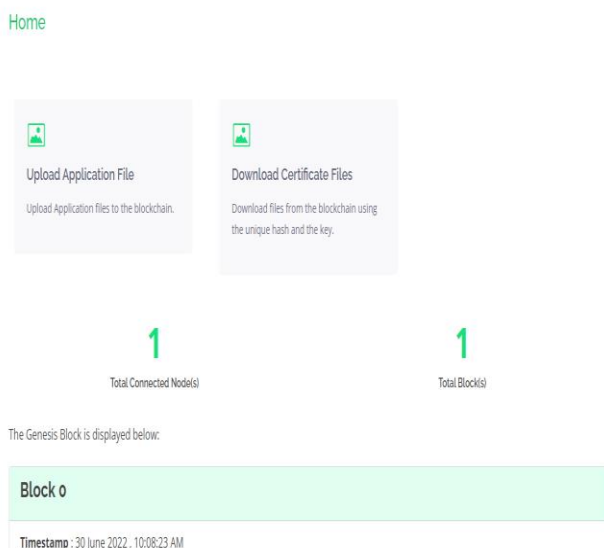


Fig. 5: user side portal for application upload and download

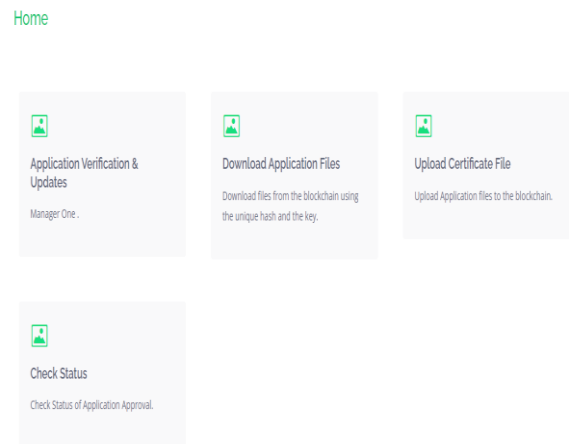


Fig. 6: Admin side portal for application certificate upload

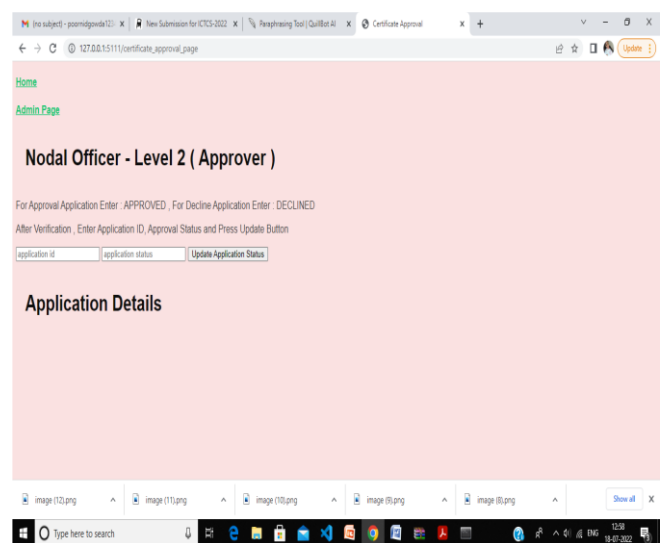


Fig. 7: officer approving the certificate

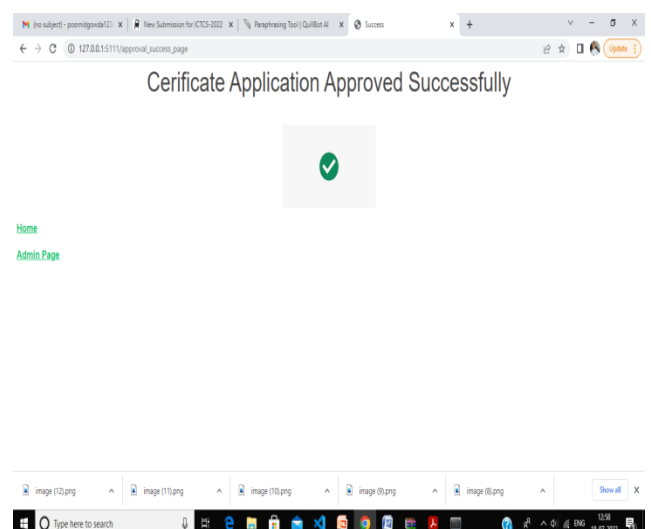


Fig. 8: Application approved successfully

V. CONCLUSION

In this research, a approach is made to identify the problem in the e-government based notarial office for the user required certificate generation, by the notarial officer with the blockchain based method of decentralized application framework of work is done to get convenient for both the user and the officer with the API grid based email for the password sharing for the certificate download.

REFERENCES

- [1.] Y. Gao, Q. Pan, Y. Liu, H. Lin, Y. Chen and Q. Wen, "The Notarial Office in E-government: A Blockchain-Based Solution," in IEEE Access, vol. 9, pp. 44411-44425, 2021, doi: 10.1109/ACCESS.2021.3066184.
- [2.] https://www.researchgate.net/publication/340647969-An_Overview_of_Blockchain_Technology_in_Government_Sectors_Use_Cases_Benefits_and_Challenges
- [3.] https://www.researchgate.net/publication/348779164-Improving_Public_Administration_by_Block_Chain_Technologies
- [4.] S. Li, W. Wei and M. Ma, "How Does E-Government Affect Corruption? Provincial Panel Evidence From China," in IEEE Access, vol. 9, pp. 94879-94888, 2021, doi: 10.1109/ACCESS.2021.3093981.
- [5.] J. Hochstetter, J. Díaz, M. Diéguez, R. Espinosa, J. Arango-López and C. Cares, "Assessing Transparency in eGovernment Electronic Processes," in IEEE Access, vol. 10, pp. 3074-3087, 2022, doi: 10.1109/ACCESS.2021.3137799.
- [6.] D. Cagigas, J. Clifton, D. Diaz-Fuentes and M. Fernández-Gutiérrez, "Blockchain for Public Services: A Systematic Literature Review," in IEEE Access, vol. 9, pp. 13904-13921, 2021, doi: 10.1109/ACCESS.2021.3052019.
- [7.] <https://dl.acm.org/doi/abs/10.1145/1693042.1693045> IJCEE 2014 Vol.6 (3): 201-206 ISSN: 1793-8163 DOI: 10.7763/IJCEE.2014.V6.822
- [8.] O. S. Al-Mushayt, "Automating E-Government Services With Artificial Intelligence," in IEEE Access, vol. 7, pp. 146821-146829, 2019, doi: 10.1109/ACCESS.2019.2946204.
- [9.] K. Gu, L. Wang and W. Jia, "Autonomous Resource Request Transaction Framework Based on Blockchain in Social Network," in IEEE Access, vol. 7, pp. 43666-43678, 2019, doi: 10.1109/ACCESS.2019.2908627.
- [10.] I. Alkrajji, "Citizen Satisfaction With Mandatory E-Government Services: A Conceptual Framework and an Empirical Validation," in IEEE Access, vol. 8, pp. 117253-117265, 2020, doi: 10.1109/ACCESS.2020.3004541.
- [11.] D. Geneiatakis, Y. Soupionis, G. Steri, I. Kounelis, R. Neisse and I. Nai-Fovino, "Blockchain Performance Analysis for Supporting Cross-Border E-Government Services," in IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1310-1322, Nov. 2020, doi: 10.1109/TEM.2020.2979325.
- [12.] F. Mohammed, A. I. Alzahrani, O. Alfarraj and O. Ibrahim, "Cloud Computing Fitness for E-Government Implementation: Importance-

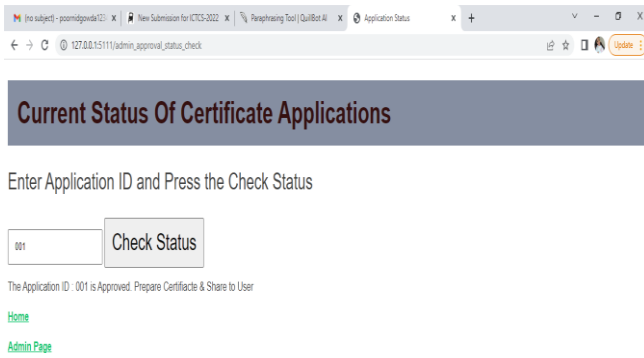


Fig. 9: approving the application check

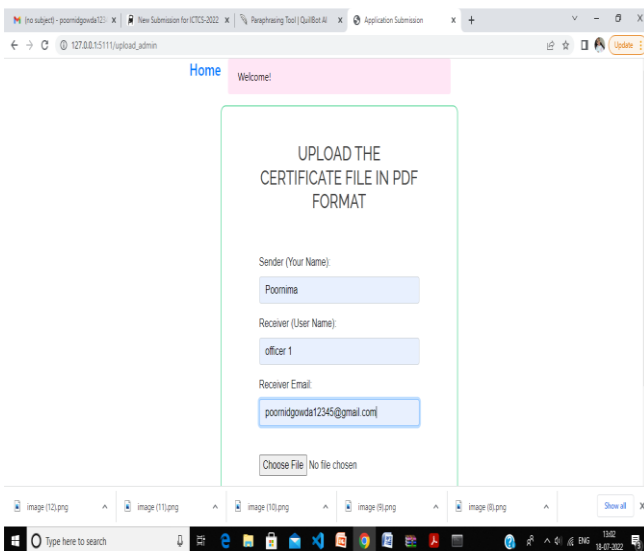


Fig. 10: uploading certificate and sending email with password

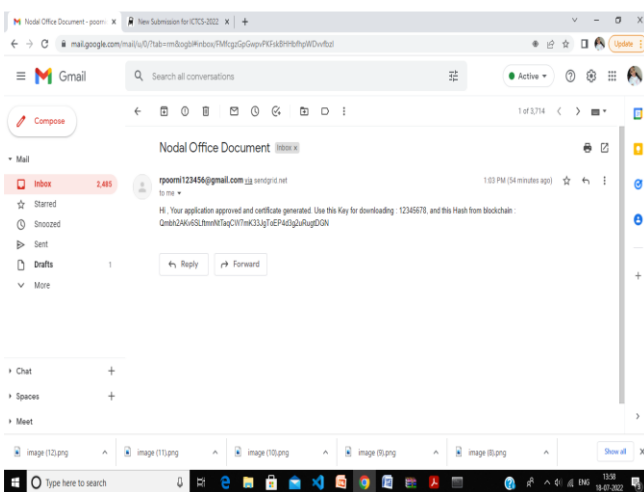


Fig. 11: email with password and status

- Performance Analysis," in IEEE Access, vol. 6, pp. 1236-1248, 2018, doi: 10.1109/ACCESS.2017.2778093.
- [13.] https://www.researchgate.net/publication/333696117_Data_model_development_for_'buying_and_selling'_transactions_as_a_real_estate_acquisition_method
- [14.] https://www.researchgate.net/publication/269406616_Big_data_framework_for_national_E-governance_plan
- [15.] M. D. Lytras and A. C. Şerban, "E-Government Insights to Smart Cities Research: European Union (EU) Study and the Role of Regulations," in IEEE Access, vol. 8, pp. 65313-65326, 2020, doi: 10.1109/ACCESS.2020.2982737.
- [16.] https://www.researchgate.net/publication/350966646_A_Systematic_Conceptual_ReviewBlockchain_As_A_Next_Generation_EGovernment_Information_Infrastructure
- [17.] Małgorzata Uhruska & Agnieszka Małkowska, 2021. "The Impact of COVID-19 on the Work of Property Valuers: A Glance at the Polish State of Play," JRFM, MDPI, vol. 14(8), pages 1-16, August.
- [18.] Z. Lv et al., "Managing Big City Information Based on WebVRGIS," in IEEE Access, vol. 4, pp. 407-415, 2016, doi: 10.1109/ACCESS.2016.2517076.
- [19.] <https://go.gale.com/ps/i.do?id=GALE%7CA641362748&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=14156555&p=AONE&sw=w>
- [20.] https://www.researchgate.net/publication/346564483_Recent_Progress_of_Blockchain_Initiatives_in_Government_A_Review_of_Asian_Countries
- [21.] R. Gacitúa, H. Astudillo, B. Hitpass, M. Osorio-Sanabria and C. Taramasco, "Recent Models for Collaborative E-Government Processes: A Survey," in IEEE Access, vol. 9, pp. 19602-19618, 2021, doi: 10.1109/ACCESS.2021.3050151.