Land transaction Management System With the use of Digital signatures

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

B.Tech.

In

Computer Science and Engineering

School of Computer Science & Engineering

Name: Nikhil Harshwardhan

Reg. No.: 20BCI0159

Name: Konark Patel

Reg. No.: 20BCI0169

Name: Prathamesh Rajesh Aundhakar

Reg. No.: 20BCI0123

ABSTRACT

The land registration system is an essential component of any government system that keeps track of land ownership records. In India, the conventional Land Registration method is a lengthy process that necessitates the verification of additional documents, causing registration to be delayed. Furthermore, this process necessitates a large number of intermediaries, increasing the number of fraudulent situations such as middlemen taking bribes to complete the process. It's also possible to make mistakes while processing land records. Corruption and disagreements are caused by a number of flaws and vulnerabilities in the current system. It is a time-consuming operation to manage transactions for land registration. It is highly insecure and vulnerable to forging land records, verification issues, middlemen, and other issues. These issues can be solved by using digital signatures for land transaction management.

Digital signatures have the ability to close these gaps and resolve concerns with land registry systems such as record tampering. We intend to develop a digital signature for each individual land plot based on the parameters in order to uniquely identify the plot. The signature will include physical and monetary measurements as well as the owner's information. We intend to develop a modified authentication system for land that is dynamic in response to minor changes in its specifics. This would make it easier to keep track of and control issues like reselling of previously sold lands. The adoption of digital signatures (cryptography) in this domain will have an impact on the land transaction management system's conveyancing process.

Keywords: Digital signature, transaction, sha-1, hashing, e-governance

1) INTRODUCTION

1.1) Theoretical Background

Land registration is a mechanism in which a government entity records ownership and land-related rights. Land documentation must be kept up to date because the land is a valuable asset. These documents serve as proof of ownership, ease transactions, and prevent fraud. Digital signatures ensure message security, allowing information to be sent from one end to another without affecting the message's or document's integrity. Every transaction in the public ledger is double-checked using consensus processes that involve the majority of the system's members. As fresh data emerges, hashing techniques are used to build and encrypt documents. As a result, once information has been entered, it cannot be changed without the assistance of a legal administrator.

Digital Signature:

A digital signature is a mathematical approach for verifying the integrity and validity of a message, software, or digital document. It's the digital counterpart of a handwritten signature or a stamped seal, but it has a lot more security built in. The purpose of a digital signature is to prevent tampering and impersonation in digital communications. Electronic papers, transactions, and digital messages can all benefit from digital signatures as proof of origin, identity, and status. They can also be used to affirm informed permission by signers. Public key cryptography, often known as asymmetric cryptography, is used to create digital signatures. Two keys are generated using a public key method such as RSA, resulting in a mathematically connected pair of keys, one private and one public. The two mutually authenticating cryptographic keys of public key cryptography are used to create digital signatures. The person who makes the digital signature encrypts signature-related data with a private key, which can only be decrypted with the signer's public key. If the recipient can't open the document using the signer's public key, there's a problem with the signature or the document. Digital signatures are verified in this way.

1.2) MOTIVATION

The most powerful driver of change in society is digitalization and the emergence of new technology. It was quite difficult to navigate all the details in regards to the assets in the previous established system if a user lost original physical agreements that operate as actual proof of ownership, or if documents were altered or damaged. As a result, we began to promote our concept of a digital signature-based land transaction system as a feasible alternative to the old system, taking into account a variety of factors.

2) LITERATURE SURVEY SUMMARY

1. **Paper:**

IEEE Transactions on Computers. Vol c-25, no. 12

Privacy and Security issues in Information Systems

By-REIN TURN, member, IEEE, AND WILLIS H. WARE, fellow, IEEE **Summary:**

Computer security includes the procedural and technical measures required to prevent unauthorized access, modification, use, and dissemination of data stored or processed in a computer system, to prevent any deliberate denial of service, and to protect the system in its entirety from physical harm. Thus, in this environment it is a serious challenge for the computer profession to devise effective solutions now.

Advantage:

Gives an idea of the problems faced by modern crypto systems.

2. **Paper:**

Information Security Journal: A Global Perspective

Taylor and Francis

Hardware Design and Implementation of ElGamal
Public-Key Cryptography Algorithm By:

Lo'ai A. Tawalbeh & Saadeh Sweidan

Summary:

This article presented a hardware implementation of ElGamal public-key cryptography (PKC) algorithm. ElGamal algorithm is considered one of the most popular cryptographic algorithms used to secure communications and data transmissions. The two basic components used in the ElGamal publickey cryptography (PKC) proposed processor, which implements the algorithm (EPKCP), were modular multiplier and modular exponentiation.

Advantage:

encrypted text EPKCP was optimally designed to have the smallest possible size. It comes in two versions, the difference between them was the internal modular multiplier used.

- Radix-2 modular

multiplier • a Radix-4

modular multiplier

Disadvantage:

Almost every known cryptography algorithm has a modified Elliptic curve version. ElGamal Elliptic Curve PKC (EEC) is a modified version of ElGamal PKC.

3. Paper:

International journal of computer mathematics, Taylor and Francis

Signature scheme with message recovery and its application

By-Malapati Raja Sekhar **Summary:**

The article begins with acknowledging previous works in the domain, and then points out the problem of private secret key sharing in case of dispute and indulgence of third party in the previous model. It demonstrates this problem with reference to Chen’s scheme of digital signature with an example and them gives a proposed scheme in which new parameter is added for the third party to verify the signature without sharing of the secret key of any one party.

Advantage:

- Model provides a solution for verification of denial of one party, by a third party without the reveal of the secret key.
- Model has received SRF award from the government of India, CISR.

Disadvantage:

- useful in future modification, of project not in current imagined form.

4. Paper:

International journal of computer mathematics, Taylor and Francis

Provably secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography

By- SK Hafizul Islam & G.P. Biswas

Department of computer science and engineering, Indian school of mines, Dhanbad 826004, Jharkhand, India accepted author version posted online: 26 Feb 2013. Published online: 10 Apr 2013.

Summary:

The article explains an overview on elliptic curve cryptography and certificateless digital signature and defines its computational problems under five definitions based on the two adversaries faced in the system. In recent times this methodology has been widely being used up as it removes the certificate managing problems as such. Also, the different attacks possible are listed under the title game.

Advantage: provides a strong security model **Disadvantage:**

- useful in future modification, of project not in current form

5. Paper:

Springer Journal

Secure electronic bills of lading: blind counts and digital signatures

By- Anastasia Pagnoni · Andrea Visconti **Summary:**

The existing proprietary solutions provided authenticity, integrity and non-repudiation but lacked in confidentiality, security rules that didn't consider insider malicious users and user lacked control over the security parameters. The proprietary solutions are based on closed software model where user does not have control over cryptographic protocols. Digital signature is a cryptographic protocol which creates an unbreakable binding between the users. **Advantage**:

Helps in understanding electronic bill and the help of digital signatures in it **Disadvantage:**

No direct connection with the topic, only a supplementary

6. Paper:

IET information security

HIDDEN IDENTITY BASED SIGNATURES

A. Kiayias H.-S. Zhou **Summary:**

But still the verifier knows that the identity negotiation has taken place between the signer and the identity manager and also the signature contains the name of the signer in encrypted format and such kind of encrypted name can be recovered by an opening authority.

Advantage:

Guides us to a understanding of better identity protection for our project as valuable transactions like land needs protection **Disadvantage:**

Implementation of this in our project will require a greater understanding of the topic.

7. Paper:

IET information security

HOW TO STRONGLY LINK DATA AND ITS MEDIUM

Philippe Bulens, Fran cois-Xavier Standaert and Jean-Jacques Quisquater.

Summary:

Securing documents is one of the most important things in this present World. There should be proper security for the documents, which means that there should be proper authentications and other proper security mechanisms. Some suggestions were given like the fingerprint could be stored on the document itself through an enciphered or encrypted or digitally signed 2D barcode or a smart chip. But a similar idea is developed in this paper that is to bind the fingerprint of the medium and the data which is lying on it.

Advantage:

Tells us about linking a unique signature to data and can be handy for the project **Disadvantage:**

Hard to implement

8. Paper:

Journal of CRYPTOLOGY, International association for Cryptologic Research

Security arguments for Digital Signatures and Blind Signatures

David Pointcheval and Jacques Stern,

Laboratoire d'Informatique, Ecole Normale Superieure. **Summary:**

As defined in the Introduction, there had been various proposals for signature schemes that were proven to be invulnerable. introduced blind signature schemes with complexity-based proof of security. In the lower placement provided by the Random Oracle model, we have provided security arguments for realistic and even eco-friendly digital signature schemes and blind signature schemes. In any case, the arguments in this article, based entirely on the Random Oracle model, are a fairly robust indication that the ordinary scheme of the corresponding schemes is most likely correct.

Advantage:

Blind digital signatures play a central role in anonymous electronic cash applications **Disadvantage:** Our scheme, while polynomial in all suitable parameters, is inefficient. Thus, it should be viewed merely as a proof of existence which should pave the way for efficient future implementations.

9. Paper:

International Review of Law, Computers & Technology

Taylor and Francis

E-government and developing countries: an overview

By: Subhajit Basu **Summary:**

E-governance is more than just a government website on the Internet. The strategic objective of egovernance is to support and simplify governance for all parties; government, citizens and businesses. The success of e-government initiatives and processes are highly dependent on government's role in ensuring a proper legal framework for their operation. A requirement fore-government processes to be introduced and adopted is their formal legal equivalence and standing with the paper process.

Advantage:

- Policy Coordination and Implementation; Delivery of services online
- Developing Citizen-centric programs as well as promoting and enhancing citizen participation

Disadvantage:

Mostly irrelevant to the topic and only helps in getting a faint idea about how our system can be implemented for governmental bodies

10. Paper:

Taylor & Francis, Cryptologia

Digital Signature Algorithms

William Stallings

Published online: 01 Oct 2013.

Summary:

The article explains various ways to creating a digital signature. It explains basic asymmetric digital signature scheme, Elgamal DSA, Schnorr DSA, NIST DSA, ECDSA and RSA-PSS DSA. Later on it compares the different types of schemes it discusses.

Advantage:

It gives an over view of the different types of digital signature algorithms available.

Disadvantage:

The paper in itself is hard to understand/ implement.

3) OVERVIEW OF THE PROPOSED SYSTEM

3.1) Aim of project :

To make a model that scrambles the land exchange model in a safer advanced climate, permitting the current framework to be improved and gotten. We mean to foster an advanced mark for every individual land plot dependent on the boundaries to extraordinarily recognize the plot. The mark will incorporate physical and financial estimations just as the proprietor's data. We plan to foster an adjusted verification framework for land that is dynamic in light of minor changes in its points of interest. This would make it simpler to monitor and control issues like exchanging of recently sold grounds. The effect that computerized marks will have on the conveyancing system has not been considered in land enrollment. One such touchy space is secure exchange of land and property subtleties, given the escape clauses in current framework it is needed to acquire a crypto framework for a safer climate. By our model we intend to utilize advanced marks to accomplish something similar. also tackle issues like unapproved exchanging, wrong arrangement. In our model we will produce two keys which will have a place with a specific plot, the mysterious key will be with the proprietor and the public key in the public authority vault office. When the exchange is done the mysterious key will be confirmed and afterward changed. Hence the pair of keys will be dynamic with its individual proprietors.

3.2) Objective

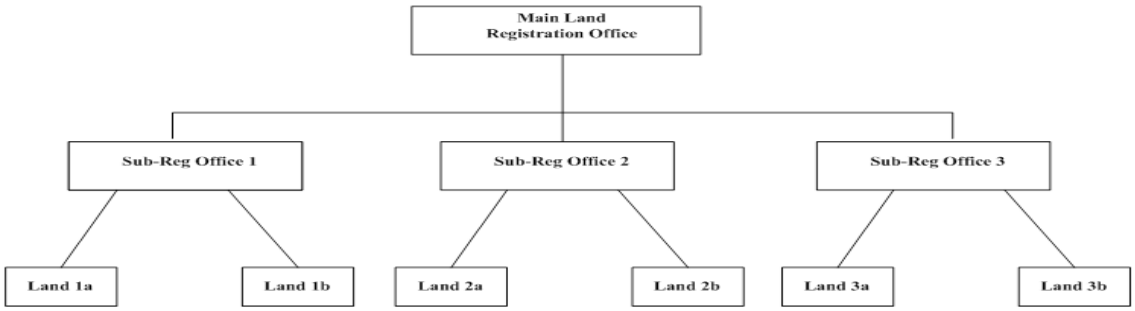
To device a model to encrypt the land transaction model in a more secure digital environment to facilitate the current system with a more enhanced and secure management system. We plan to create a digital signature for each individual land plot given the details and uniquely identify the plot, where the signature will have details of physical measure and monetary measure along with owner details. We plan to create a modified authentication for land which is dynamic to a small change in its details. This would help to keep a track and leash on problems such as reselling of already sold lands. Introduction of digital signatures in this domain will have on the conveyancing process has not been addressed in land registration.

3.3) Introduction and Related Concepts

Digital Signatures

A computerized mark is an electronic mark that can be utilized to confirm the character of the sender of a message or the underwriter of a report, and to guarantee that the first substance of the message or archive that has been sent is unaltered. Computerized marks are effectively movable, can't be imitated by another person, and can be consequently time-stepped. A computerized mark can be utilized with any sort of message, regardless of whether it is encoded or plaintext. Hence Digital Signatures give the accompanying three highlights: -

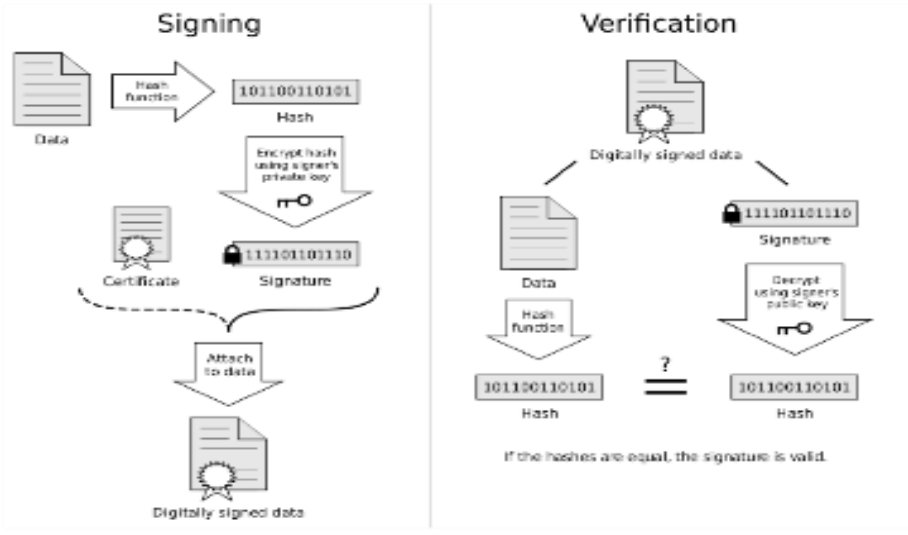
1. **Confirmation Digital** marks are utilized to verify the wellspring of messages. The responsibility for computerized signature key is bound to a particular client and hence a legitimate mark shows that the message was sent by that client.
2. **Integrity** - In numerous situations, the sender and beneficiary of a message need affirmation that the message has not been modified during transmission. Computerized Signatures give this component by utilizing cryptographic message digest capacities
3. **Non-Repudiation:** Computerized marks guarantee that the sender who has marked the data can't sometime in the future deny having marked it



Digital signature work:

The Public and Private Keys are required for Digital Signatures (awry key sets, numerically connected gigantic numbers). Cryptography uses encryption and unscrambling in the same way that physical keys are used for locking and unlocking. The private key is usually kept secret with the owner on a secure medium such as a crypto smart card or a crypto token. Everyone has access to the public key. Data scrambled by a private key must be decoded using the public key associated with it.

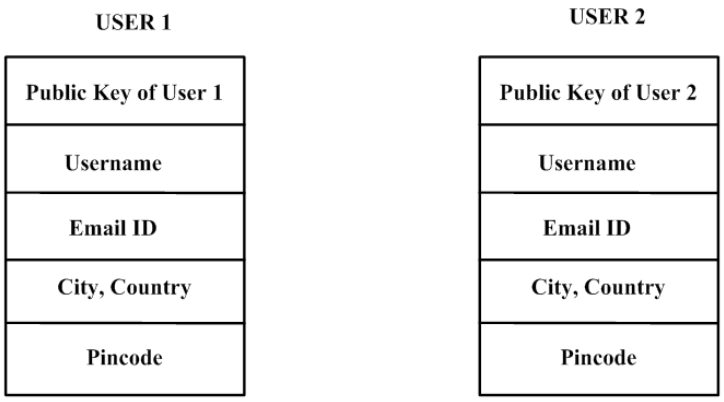
The client sends his or her Private Key to digitally sign an electronic record. The recipient uses the recipient's Public Key to validate the digital signature.



Land enrollment includes assortment of subtleties like proprietorship and size of the property. At present the whole cycle Land enrollment includes assortment of subtleties like proprietorship and size of the property. The fundamental issue with the previously mentioned strategy for land library upkeep is that any future reference that necessities

The principal issue with the previously mentioned strategy for land library support is that any future reference that should be taken from these printed versions will include a lot of work. This interaction is tedious. A few methodologies have been made to computerize the land library information upkeep by killing the most common way of keeping scholarly records. This is at first done by putting away the information in colossal data sets. Be that as it may, such a strategy isn't productive as far as information security as the information substance are penetrated effectively as information altering can occur if there should be an occurrence of inadequately kept up with data sets.

Digital signature is a distributed ledger system that maintains a previous record of all transactions over a peer-to-peer system. Using digital signature to implement a land register helps to avoid illegal transactions, making the system safer. Because it is difficult to copy the digital signature, utilising this technology to construct a land register helps to avoid any illicit land transactions. Contracts and ownership information are kept in a decentralized manner. Because the digital signature implementation eliminates the need for physical interaction, it is easier to track data transactions and thus increases overall security for system users. Blockchain offers the possibility of establishing a solid digital identity system. Each block in the digital signature represents the data involved in a land transaction.
It also features the display of past transaction details, financial institution information, data protection, and fault tolerance without data loss.



Every client's public key will be accessible in a disseminated way all through the organization. People will utilize their private key to go into their foundation and choose how much land should be sold and how

much cash should be conveyed to the customers. During an exchange, the public key is sent across the organization for agreement, while the private key guarantees that the individual doing the exchange can do as such securely.

3.4) Framework, Architecture or Module for the Proposed System

```
import hashlib
import random
import sys import
fileinput

r = 0 s =
0

def modinv(a,m):     a =
a%m     for x in
range(1,m):         if((a*x)
% m == 1):
            return(x)
    return(1)

def isprime(num):
    for n in range(2,int(num**1/2)+1):
if num%n==0:             return False
    return True

def hasher(message):     hash_val =
hashlib.sha1(message.encode("UTF-
8")).hexdigest()
    return hash_val

def primesInRange(x, y):
prime_list = []     for n in
range(x, y):         isPrime =
True

        for num in range(2, n):
      if n % num == 0:
isPrime = False

    if isPrime:
prime_list.append(n)
  return prime_list

while(1):     pl =
primesInRange(101,999)     p
= random.choice(pl)

  temp=[]     for q in range(2,p):         if ((p-
1)%q == 0) and isprime(q) and q>9:
        temp.append(q)
if(len(temp) != 0):
    break

q=temp[0]
flag = True
while(flag)
:
  h=random.randint(1,(p-1))
if(1<h<(p-1)):         g=1
while(g==1):             g =
pow(h,int((p-1)/q)) % p
flag = False     else:
      print('Invalid
Entry')
x=random.randint(1,
(q-1)) y = (g**x) % p
def
signature(name,p,q,g,x
):     with open(name)
as file:         text =
file.read()
hash_comp =
hasher(text)     r = 0
s = 0     while(s==0 or
r==0):
k=random.randint(1,(q
-1))         r =
((pow(g,k))%p)%q
i = modinv(k,q)
hashed =
int(hash_comp,16)
s = (i*(hashed+(x*r)))
% q     return(r,s,k) def
verification(name,p,q,g
,r,s,y):     with
open(name) as file:
text = file.read()
hash_comp =
hasher(text)         w =
modinv(s,q)
hashed =
int(hash_comp,16)
u1 = (hashed*w) % q
u2 = (r*w) % q         v
=
((pow(g,u1)*pow(y,u2
))%p)%q
if(v==r):
return(1)         else:
return(0) print()

    class buffer():

        def __init__(self,r,s,owner_name):
```

```
        self.r = r
    self.s = s
        self.owner_name = owner_name


    argv = []


    comp1 = signature(r'C:\Users\hp\Desktop\crypto
    project\Land_1.txt',p,q,g,x)


    argv.append(buffer(comp1[0],comp1[1],'Yash
    Dahiya')) comp2 =
    signature(r'C:\Users\hp\Desktop\crypto
    project\Land_2.txt',p,q,g,x)


    argv.append(buffer(comp2[0],comp2[1],'Adhi SD'))


    def transaction():
       print("in database: land1 land2")
    land_index=int(input("enter the land you want to
    access (1 for land 1 and similarly):"))
    onr_nam=input("enter owner name: ")
    onr_id=input("enter owner id: ")
    if(argv[land_index-1].owner_name==onr_nam):
    doc=input("enter the documents: ")
    temp=verification(doc, p, q, g, argv[land_index-
    1].r, argv[land_index-1].s, y)        if(temp==1):
            print("the document is valid")
    print("the transaction is verified, proceed with
    payment\n")
            print("\npayment sucessful\n")
    new_onr=input("enter the new owner name: ")
    new_id=input("enter new owner id: ")
    old_data=
    hasher(onr_nam+str(argv[land_index1].r)+str(argv[
    land_index-1].s)+"transaction")          count=0
    for i, line in enumerate(fileinput.input(doc,
    inplace=1)):
            count=count+1
sys.stdout.write(line.replace(onr_nam,
new_onr))              if
count == 27:
              sys.stdout.write("\n")
sys.stdout.write(old_data)          for i, line in
enumerate(fileinput.input(doc, inplace=1)):
            sys.stdout.write(line.replace(onr_id,
new_id))          print("the document is modified for
future use")          tmp_sign=signature(doc,p,q,g,x)
argv[land_index-1].r=tmp_sign[0]
argv[land_index-1].s=tmp_sign[1]
argv[land_index-1].owner_name=new_onr
print("the data base is updated")        else:
         print("invalid document, modification
occured.\n")     else:
      print("invalid owner name")
   print()
return("")
```

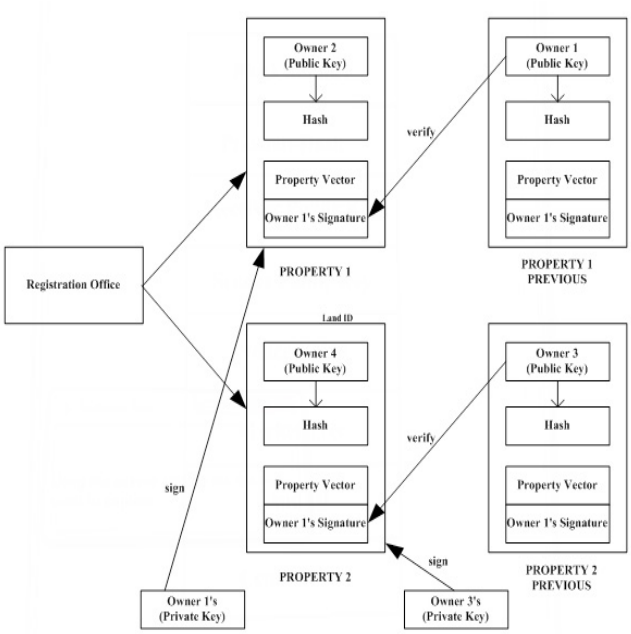
```
def exchange():     print("in database: land1 land2")
land_1=int(input("enter the first land you want to
access (1 for land 1 and similarly):"))
onr_1=input("enter owner name for first land: ")
onr_id_1=input("enter the owner id for first land: ")
land_2=int(input("\n enter the second land you want
to access (1 for land 1 and similarly):"))
onr_2=input("enter owner name for second land: ")
onr_id_2=input("enter the owner id for second land:
")     if(argv[land_1-1].owner_name==onr_1 and
argv[land_2-1].owner_name==onr_2):        #main
code here        doc1=input("enter the documents for
first land: ")        temp1=verification(doc1, p, q, g,
argv[land_1-1].r, argv[land_1-1].s, y)
      doc2=input("enter the documents for second
land: ")        temp2=verification(doc2, p, q, g,
argv[land_2-1].r, argv[land_2-1].s, y)
if(temp1==1 and temp2==1):
          print()
          print("the documents are valid and
verified")          print()          print("proceed
with excange")          old_1=
hasher(onr_1+str(argv[land_11].r)+str(argv[lan
d_1-1].s)+"exchange")          count1=0
for i, line in enumerate(fileinput.input(doc1,
inplace=1)):
            count1=count1+1
sys.stdout.write(line.replace(onr_1, onr_2))
if count1 == 27:
              sys.stdout.write("\n")
sys.stdout.write(old_1)          for i, line in
enumerate(fileinput.input(doc1, inplace=1)):
              sys.stdout.write(line.replace(onr_id_1,
    onr_id_2))
          print("document of first land is
    updated")          #argv[land_2-
    1].owner_name=onr_1          old_2=
    hasher(onr_2+str(argv[land_21].r)+str(argv[la
    nd_2-1].s)+"exchange")          count2=0
    for i, line in enumerate(fileinput.input(doc2,
    inplace=1)):
              sys.stdout.write(line.replace(onr_2,
    onr_1))              count2=count2+1              if
    count2 == 27:
                sys.stdout.write("\n")
    sys.stdout.write(old_2)          for i, line in
    enumerate(fileinput.input(doc2, inplace=1)):
              sys.stdout.write(line.replace(onr_id_2,
    onr_id_1))
          print()
          print("document of second land is
    updated")
          print()
          print("documents updated for future
    use")
          print()
          tmp_sign1=signature(doc1,p,q,g,x)
    argv[land_1-1].r=tmp_sign1[0]
    argv[land_1-1].s=tmp_sign1[1]
```

```
    argv[land_1-1].owner_name=onr_2
    print("first land database udated")
    tmp_sign2=signature(doc2,p,q,g,x)
    argv[land_2-1].r=tmp_sign2[0]
    argv[land_2-1].s=tmp_sign2[1]
```

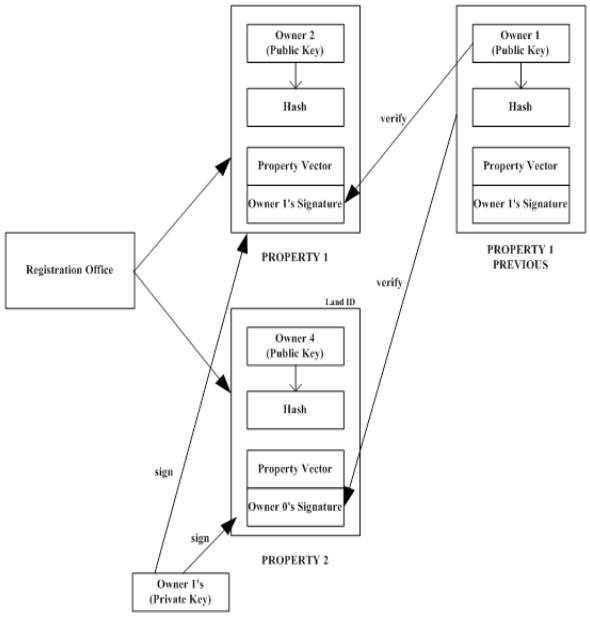
3.5) Proposed System Model

```
        argv[land_2-1].owner_name=onr_1
        print("second land database updated")
        print()
print("exchange sucessful")
elif(temp1==0 and temp2==1):
        print("document of first land is modified")
elif(temp1==1 and temp2==0):
print("documnet of second land is modified")
else:
        print("both documents are modified")
elif(argv[land_1-1].owner_name!=onr_1 and
argv[land_2-1].owner_name==onr_2):
      print("owner of first land is invalid")
elif(argv[land_1-1].owner_name==onr_1
and argv[land_2-1].owner_name!=onr_2):
print("owner of second land is invalid")
else:
      print("invalid owners")
return()

while(1):
   print('****MENU****')
print('\n1.Transaction\n2.Exchange\n3.exit\
n')    ch = int(input('Enter your choice: '))
if (ch==3):        print('Thanks')        break
elif (ch==2):        exchange()
elif(ch==1):        transaction()    else:
print("invalid")
```



EXCHANGE – Block Diagram



TRANSACTION – Block Diagram

4) Proposed System Analysis and Design:

The program is an application of Digital Signature Algorithm(DSA), which serves as the Backend. Digital signatures use the PKI standard and the Pretty Good Privacy (PGP) encryption program because both reduce potential security issues that come with transmitting public keys, in this case the document for the respective lands. Validating that the seller's document belongs to that individual and verify the seller's ownership.

Next there is a buffer/archive which stores the signatures along with the owner name of the lands. The program implements a simple linear search inorder to identify the land being dealt with. The complexity for the search algorithm is O(n).

The program offers two functions: one is the Transaction and the other one is the Exchange of lands. They run over the backend of Verification of the DSA.

And once it is verified it uses file handling module Sys and Fileinput, then it modifies the document as per the new ownership details along with a special hash appended to it at the end of the document to prevent forgery. The File handling also run over the linear search having complexity O(n).

5) RESULTS AND DISCUSSIONS

Once executed the program provides the user with a menu with the Transaction , Exchange and exit options. As per the selected operation the program proceeds.

Case1: Transaction

A list of land in the database will appear out of which the one interested is to be selected. After selection the program will ask for the current owner name and the owner id which once verified leads to input of documents which are again verified. Then proceeded by payment and input for the new owner name and owner id. the documents are modified accordingly and a special hash is also appended at a defined location in the document.

Case2: Exchange

A list of land in the database will appear out of which the two interests are to be selected. After selection the program will ask for the current owner name and the owner id of both the lands in sequence. Once both are verified it leads to input of documents which are again verified. Then proceeded by the modification of documents accordingly and a special hash is also appended at a defined location in the documents.

Case3: Exit

The exit ends the whole server of the program cancelling all changes made and reverts the whole database to first owners. Printing a thanks message for the user end.

Few Problems and Bugs:

- In the DSA in some cases there is a problem while calculating the value of ‘g’ due to the use of the random library which causes errors in computation.
- In some cases even though the entered document is wrong the values of ‘v’ and ‘r’ may be same or matched by fluke or extreme case, so in this anomaly the wrong document will be taken as valid document. Hindering the credibility of the program.

Reference:

Weblinks:

1. https://www.techtarget.com/searchsecurity/definition/digital-signature
2. https://www.includehelp.com/cryptography/digital-signature-algorithm-dsa.aspx
3. https://www.geeksforgeeks.org/constructors-inpython/#:~:text=Constructors%20are%20generally%20used%20for,when%20an%20object%20is%20created.
4. https://stackoverflow.com/questions/125703/how-to-modify-a-text-file
5. https://github.com/Abhiramborige/Crypto-systems/blob/master/digital_signature.py

Journal:

1. R. Turn, W. H . Ware, 'Privacy and Security issues in Information Systems', IEEE Transactions on Computers,(1976) Vol c-25, no. 12
2. Lo'ai A. Tawalbeh, Saadeh Sweidan, 'Hardware Design and Implementation of ElGamal Public-Key Cryptography Algorithm', Information Security Journal: A Global Perspective, (2010), Taylor and Francis
3. International journal of computer mathematics, Taylor and Francis, Signature scheme with message recovery and its application, Malapati Raja Sekhar
4. International journal of computer mathematics, Taylor and Francis, Provably secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography, SK Hafizul Islam & G.P. Biswas
5. Springer journal, Secure electronic bills of lading: blind counts and digital signatures, Anastasia Pagnoni · Andrea Visconti
6. IET information security ,HIDDEN IDENTITY BASED SIGNATURES,A. Kiayias H.-S. Zhou
7. IET information security,HOW TO STRONGLY LINK DATA AND ITS MEDIUM ,Philippe Bulens, Fran cois-Xavier Standaert and Jean-Jacques Quisquater.
8. Journal of CRYPTOLOGY, International association for Cryptologic Research ,Security arguments for Digital Signatures and Blind Signatures*,David Pointcheval and Jacques Stern
9. International Review of Law, Computers & Technology Taylor and Francis ,E-government and developing countries: an overview, Subhajit Basu
10. Taylor & Francis, Cryptologia, Digital Signature Algorithms, William Stallings