

INFORMATION SECURITY MANAGEMENT

(J-Component)

WINTER SEMESTER 2022-2023

PROJECT REPORT

TITLE

**SECURE LAND TRANSACTION MANAGEMENT SYSTEM
WITH THE USE OF DIGITAL SIGNATURE**

TEAM MEMBERS:

NIKHIL HARSHWARDHAN - 20BCI0159

SELVA KRISHNAN - 20BCI0268

VINEETH KRISHNA - 20BDS0387

ABILASH - 20BDS0408

SUBMITTED TO

- Prof. SELVI M (SCOPE)



VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

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.

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

INTRODUCTION:

1.1 OVERALL IDEA OF THE PROJECT

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.

1.2 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.

1.3 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.

1.4 STATISTICS RELATED TO THE METHODS USED

The security of digital signature algorithms is usually evaluated by the number of operations required to break the algorithm. This is usually measured in terms of time and computational resources required to perform these operations.

One common metric used to evaluate the security of digital signature algorithms is the number of operations required to forge a signature. This is known as the signature forgery attack. For example, the Elliptic Curve Digital Signature Algorithm (ECDSA) is considered secure as long as the key length is greater than 256 bits, as the number of operations required to forge a signature is infeasible with current computational resources.

In addition to these metrics, digital signature algorithms are also evaluated based on their resistance to other attacks, such as the man-in-the-middle attack, replay attack, and chosen message attack. The security of a digital signature algorithm also depends on the secure management of the private keys and the use of secure random number generators.

Some commonly used Digital Signature Algorithms include:

- RSA: RSA is one of the most widely used public key cryptography algorithms and is commonly used for digital signatures. It's widely used in various applications such as SSL/TLS certificates, code signing, and secure email.
- DSA: The Digital Signature Algorithm (DSA) is a US government standard for digital signatures and is widely used in the financial industry for secure transactions.
- ECDSA: The Elliptic Curve Digital Signature Algorithm (ECDSA) is an efficient variant of DSA that uses elliptic curve cryptography. ECDSA is widely used in blockchain and cryptocurrency applications due to its fast signature generation and verification times.
- PGP: Pretty Good Privacy (PGP) is a widely used encryption and digital signature software that uses a combination of RSA and DSA algorithms. PGP is commonly used for secure email communication and file encryption.

OVERVIEW OF THE PROPOSED SYSTEM:

2.1) 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 (cryptography) 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.

2.2) 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 (cryptography) in this domain will have on the conveyancing process has not been addressed in land registration.

2.3) INTRODUCTION AND RELATED CONCEPTS

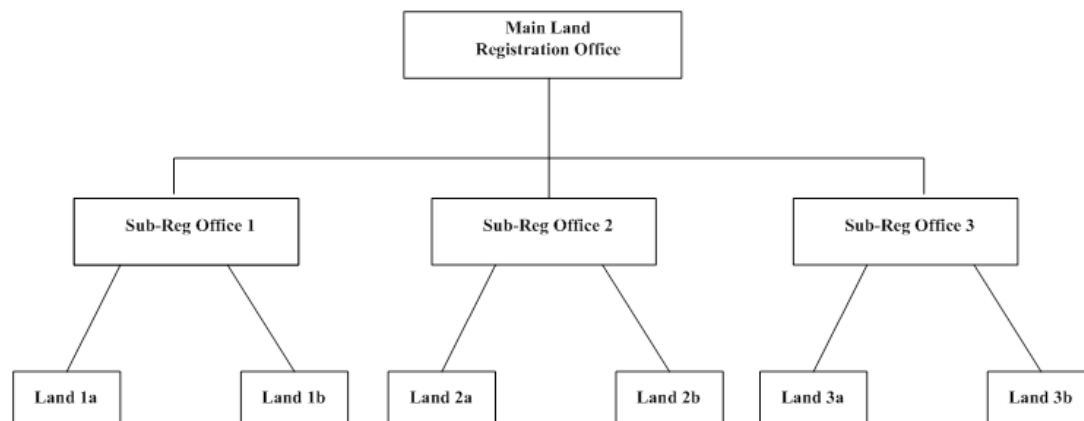
DIGITAL SIGNATURES

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

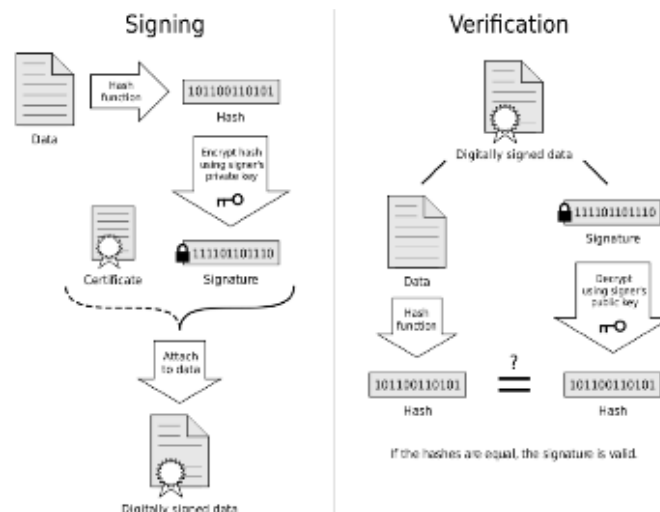
3. Non-Repudiation: Computerized marks guarantee that the sender who has marked the data can't sometime in the future deny having marked it



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.

USER 1	USER 2
Public Key of User 1	Public Key of User 2
Username	Username
Email ID	Email ID
City, Country	City, Country
Pincode	Pincode

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.

LITERATURE SURVEY:

S.no	Paper	Summary	Advantages	Disadvantages
1.	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	<p>Legal provisions already exist to require data security in personal information record-keeping systems. Valuable organizational assets are increasingly represented by records in computer databases rather than by hardcopy documents; systems such as the Electronic Fund Transfer offer high-payoff opportunities for computer crime of various kinds. Computer security includes the procedural and technical measures required</p> <p>1) to prevent unauthorized access, modification, use, and dissemination of data stored or processed in a computer system,</p> <p>2) to prevent any deliberate denial of service, and</p> <p>3) 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</p>	Gives an idea of the problems faced by modern crypto systems.	-
2.	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	<p>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.</p> <p>The two basic components used in the ElGamal public-key cryptography (PKC) proposed processor, which implements the algorithm (EPKCP), were modular multiplier and modular exponentiation.</p>	<p>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.</p> <ul style="list-style-type: none">• Radix-2 modular multiplier• a Radix-4 modular multiplier	Almost every known cryptography algorithm has a modified Elliptic curve version. ElGamal Elliptic Curve PKC (EEC) is a modified version of ElGamal PKC

3.	<p>International journal of computer mathematics, Taylor and Francis</p> <p>Signature scheme with message recovery and its application By- Malapati Raja Sekhar Applied statistics unit, Indian statistical Institute, Kolkata 108, India</p>	<p>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.</p> <p>It demonstrates this problem with reference to Chen's scheme of digital signature with an example and then 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.</p>	<ul style="list-style-type: none"> • 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 the SRF award from the government of India, CISR. 	useful in future modification, of project not in current imagined form.
4.	<p>International journal of computer mathematics, Taylor and Francis</p> <p>Provably secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography By- SK Hafizul Islam & G.P. Biswas</p> <p>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.</p>	<p>The article explains an overview on elliptic curve cryptography and certificateless digital signature and defines it's 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.</p> <p>Type 1: adversary A1 cannot access the master key but alter public key.</p> <p>Type 2: adversary A2 cannot access the public key but alter master key. Also, the different attacks possible are listed under the title game. Later on, the article proposes a model to fix all these issues using a partial private key extract and listed procedures</p>	provides a strong security model	-

5.	<p>Springer journal Secure electronic bills of lading: blind counts and digital signatures By Anastasia Pagnoni · Andrea Visconti</p>	<p>The existing proprietary solutions provided authenticity, integrity and nonrepudiation but lacked in confidentiality, security rules that didn't consider insider malicious users and user lacked control over the security parameters. Malicious insider user was able to read encrypted data after the decryption by Bolero platform and create fake message. So it is prone to insider fraud. The proprietary solutions are based on closed software model where user does not have control over cryptographic protocols.</p> <p>Digital signature is a cryptographic protocol which creates an unbreakable binding between the users. It protects the transmission of messages and provide authentication, non-repudiation and integrity.</p>	<p>Helps in understanding electronic bill and the help of digital signatures in it</p>	<p>No direct connection with the topic, only a supplementary</p>
6.	<p>IET information security HIDDEN IDENTITY BASED SIGNATURES A. Kiayias H.-S. Zhou Department of computer science and engineering, University of Connecticut, Storrs, CT 06269, USA</p>	<p>In this Hidden identity based signatures, a signer obtains his/her signing key by having a communication with the identity manager and he/she will negotiate his/her identity with the identity manager. With the given secret-key the signer can produce signatures on a message so that his/her identity is not revealed to the verifier.</p> <p>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.</p>	<p>Guides us to a understanding of better identity protection for our project as valuable transactions like land needs protection</p>	<p>Implementation of this in our project will require a greater understanding of the topic.</p>

7.	<p>IET information security HOW TO STRONGLY LINK DATA AND ITS MEDIUM Philippe Bulens, Francois Xavier Standaert and Jean Jacques Quisquater. Université catholique de Louvain, B-1348 Louvain-la-Neuve.</p>	<p>Securing documents is one of the most important thing 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. Like in the print signature, the idea is achieved by performing digital signature on these information as a whole. But contrary to where the fingerprint is printed on the paper and these are analyzed using shape matching methods, we make the fingerprint intrinsic to the paper. For this, we use ultraviolet fibers during the fabrication process of the paper. The expected solution depends on the combination of a physically unclonable function with robust cryptography and randomness extraction schemes, etc.</p>	<p>Tells us about linking a unique signature to data and can be handy for the project</p>	<p>Hard to implement</p>
8.	<p>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 Supérieure.</p>	<p>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.</p>	<p>Blind digital signatures play a central role in anonymous electronic cash applications</p>	<p>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.</p>

9.	International Review of Law, Computers & Technology Taylor and Francis E-government and developing countries: an overview By: Subhajit Basu	E-governance is more than just a government website on the Internet. The strategic objective of e-governance 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 for government processes to be introduced and adopted is their formal legal equivalence and standing with the paper process.	<ul style="list-style-type: none"> • Policy Coordination and Implementation; Delivery of services online • Developing Citizencentric programs as well as promoting and enhancing citizen participation 	Mostly irrelevant to the topic and only helps in getting a faint idea about how our system can be implemented for governmental bodies
10.	Taylor & Francis, Cryptologia Digital Signature Algorithms William Stallings Published online: 01 Oct 2013.	The article explains various ways to create a digital signature. It explains basic asymmetric digital signature schemes, Elgamal DSA, Schnorr DSA, NIST DSA, ECDSA and RSA-PSS DSA. Later on it compares the different types of schemes it discusses.	It gives an overview of the different types of digital signature algorithms available	The paper in itself is hard to understand/ implement.
11.	An Approach to Secure Land Transactions using Digital Certificates and Public Key Infrastructure by M. Chen et al.	The paper proposes a method for securing land transactions using digital certificates and public key infrastructure (PKI), which involves assigning digital certificates to landowners, verifying their identities and ownership of land, and storing the certificates in a central database. Smart contracts can also be used to automate the process of land transactions. The proposed method is evaluated using a case study in China.	Increased security in land transactions. Improved transparency and efficiency. Reduces the risk of fraud and manipulation	Requires a significant investment in technology infrastructure. Requires a high level of technical expertise to implement
12.	An Efficient and Secure Land Transaction System using Public Key Cryptography by Y. Zhang et al	The paper proposes a land transaction system that uses public key cryptography to secure land ownership records and prevent fraudulent transactions. The system uses a distributed ledger technology (DLT) to store land records and smart contracts to automate the transaction process. The proposed system is evaluated using simulations and experiments.	Increased security and accuracy of land ownership records. Improved efficiency of land transactions. Can be used to automate the process of land transactions.	Requires a significant investment in technology infrastructure. May require significant changes to existing land registration systems.

13.	A Proposed Framework for Secure Land Transactions using Cryptographic Algorithms by K. Liu et al.	The paper proposes a framework for securing land transactions using cryptographic algorithms, including a combination of symmetric and asymmetric encryption algorithms, and the use of smart contracts to automate the transaction process. The proposed framework is evaluated using simulations and experiments.	Increased security and accuracy of land ownership records. Can be customized to suit the specific needs of different regions	Requires a high level of technical expertise to implement. Requires a significant investment in technology infrastructure
14.	A Study on the Security of Land Transactions using Digital Signatures by Y. Park et al	The paper examines the use of digital signatures for securing land transactions, proposing a model that assigns a unique digital signature to each landowner to verify the authenticity of their ownership records and transaction details. The proposed model is evaluated using simulations and experiments.	Increased security and accuracy of land ownership records. Reduced risk of fraud and manipulation.	Requires a high level of technical expertise to implement. May require significant changes to existing land registration systems
15.	A Digital Signature-Based Security Framework for Land Registration Systems by T. Hu et al.	The paper proposes a digital signature-based security framework for land registration systems, which ensures the confidentiality, integrity, authentication, and non-repudiation of land transaction data. The framework uses digital signatures as the primary security mechanism, and it involves the creation of digital certificates, key management, and a secure communication protocol to facilitate secure land transactions.	Provides a secure and reliable land registration system Ensures the authenticity and integrity of transaction data Provides confidentiality, authentication, and non-repudiation of land transaction data	Implementation and maintenance of the framework could be complex and expensive Dependence on digital signatures could create a single point of failure if the signature key is compromised

16.	A Blockchain-Based Land Transaction System with Smart Contract by J. Li	The research paper proposes a blockchain-based land transaction system with smart contracts to enhance the security and efficiency of land transactions.	<p>1. The use of blockchain ensures the immutability and transparency of transaction records.</p> <p>2. Smart contracts automate and enforce the terms of the transaction.</p> <p>3. The system is decentralized, reducing the risk of fraud and corruption.</p>	<p>1. The use of blockchain can lead to slower transaction times due to the consensus process.</p> <p>2. The system may require significant computational resources to maintain.</p>
17.	A Survey on Blockchain for Secure Land Administration by M. Morales et al.	The paper provides a comprehensive survey of the use of blockchain technology in secure land administration, highlighting its potential benefits and limitations. The authors review various blockchain-based land administration systems and explore the potential of blockchain for addressing the challenges in land administration, such as land tenure security, corruption, and inefficiencies.	<p>Offers a secure, transparent, and tamper-proof system for land administration</p> <p>Provides an immutable record of land transactions and ownership information</p> <p>Reduces the risk of fraud, corruption, and errors in land transactions</p> <p>Enables more efficient and cost-effective land administration processes</p> <p>Supports decentralized and peer-to-peer transactions, reducing the need for intermediaries</p>	<p>Requires a significant upfront investment in technology and infrastructure</p> <p>Faces challenges in integrating with existing land administration systems and legal frameworks</p> <p>Raises concerns about data privacy and confidentiality</p> <p>Requires a consensus mechanism for validating transactions, which can be slow and energy-intensive</p> <p>Faces scalability issues when dealing with large-scale land administration systems</p>

18.	Secure Land Transactions using Blockchain Technology by S. S. Sunkavalli et al.	The paper proposes a blockchain-based system for secure land transactions, which provides transparency, immutability, and tamper-resistance. The system uses a smart contract to automate the process and ensures data integrity using cryptographic techniques.	Provides tamper-resistance and data immutability through the use of blockchain technology. Ensures transparency and traceability of land transactions.	The adoption of blockchain technology in land transactions requires significant changes in the existing legal and administrative frameworks.
19.	A Secure Land Registration System using Blockchain Technology by M. El-Hajj et al.	The paper proposes a blockchain-based land registration system that provides security, transparency, and accessibility for all parties involved in the process. The system is designed to prevent fraudulent activities and ensure the authenticity of transactions. It uses smart contracts to automate processes and reduce costs.	Provides a secure and transparent system for land registration Prevents fraudulent activities and ensures the authenticity of transactions Uses smart contracts to automate processes and reduce costs	The system may require a significant investment in infrastructure and training Blockchain technology is still in its early stages and may not be widely adopted yet
20.	A Novel Blockchain-based Land Tenure System for Secure Land Transactions by Y. Huang et al.	The paper proposes a blockchain-based land tenure system that can ensure secure land transactions by providing tamper-proof records and transparency. The proposed system consists of three layers: a blockchain layer, a service layer, and an application layer. The system's smart contracts automatically execute land transactions, eliminating the need for intermediaries.	Provides tamper-proof records and transparency Eliminates the need for intermediaries Smart contracts automatically execute land transactions	The proposed system's scalability needs to be further tested and evaluated. The system may face legal challenges in some jurisdictions where the use of blockchain technology for land registration is not yet recognized.

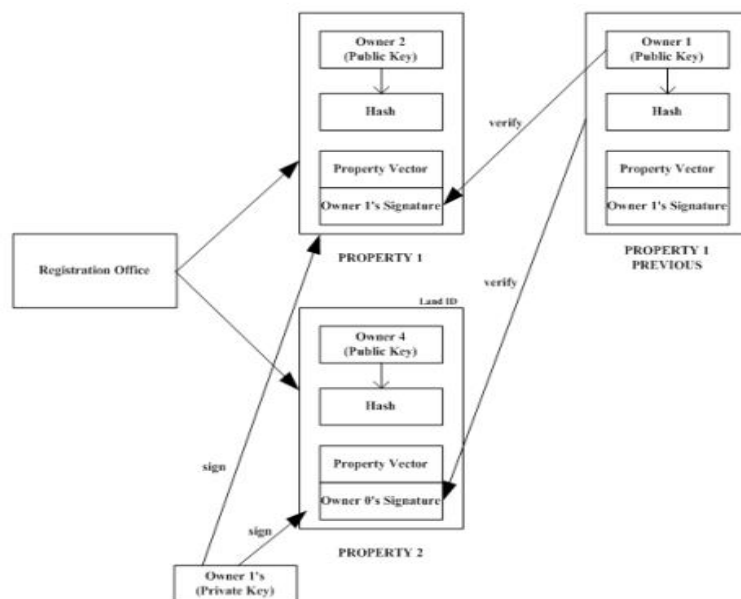
PROPOSED METHODOLOGY:

Digital Signature Algorithm

- Private Key Calculation: Choose a random number x in the range 1 to $q-1$.
 - Public Key Calculation: Calculate $y = g^x \bmod p$.
 - Signature Generation: Given a document D , calculate the hash value $H(D)$. Choose a random number k in the range 1 to $q-1$. Calculate $r = (g^k \bmod p) \bmod q$ and $s = ((H(D) + x*r) * k^{-1}) \bmod q$.
 - Signature Verification: Given a signature (r, s) and a document D , calculate the hash value $H(D)$. Calculate $w = s^{-1} \bmod q$. Calculate $u1 = (H(D) * w) \bmod q$ and $u2 = (r * w) \bmod q$. Calculate $v = ((g^{u1} * y^{u2}) \bmod p) \bmod q$. If $v = r$, then the signature is valid.
1. **Key Generation:** The first step is to generate a public/private key pair for each party involved in the transaction. The private key is kept secret and used to sign the transaction, while the public key is used to verify the signature. Generate a private key x , where x is a random number in the range 1 to $q-1$. Calculate the public key y as $y = g^x \bmod p$.
 2. **Preparation of the Transaction:** The next step is to prepare the transaction, which typically involves creating a digital document that outlines the terms and conditions of the transaction.
 3. **Signing the Transaction:** The transaction is then signed using the private key of the sender. This creates a digital signature that can be verified using the public key of the sender. To sign a document, the signer calculates the hash value of the document and uses their private key x and a random number k to calculate two values r and s . The signature is (r, s) .
 4. **Verification of the Signature:** The recipient verifies the signature using the public key of the sender. This ensures that the transaction was sent by the sender and has not been tampered with in transit. To verify the signature, the verifier calculates the hash value of the document and uses the signer's public key y , the signature (r, s) and the hash value to calculate the values $u1$, $u2$ and v . If $v = r$, then the signature is valid.
 5. **Storage and Retention:** The signed transaction is then stored securely for future reference and retention.
 6. **Validation of the Transaction:** The transaction is then validated by a trusted third-party, such as a land registry, to ensure that the transaction is legitimate and complies with local laws and regulations.
 7. **Finalisation of the Transaction:** Upon successful validation, the transaction is considered final and the transfer of ownership is recorded on the land registry.

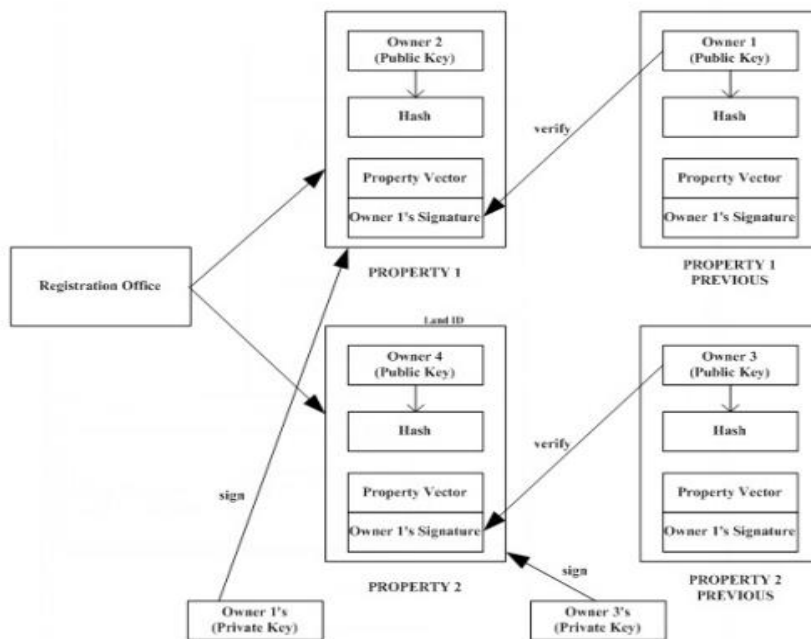
ARCHITECTURAL DIAGRAM:

Transaction Block diagram



1. The module first prints a message showing the available lands in the database, which in this case are land1 and land2.
2. The user is asked to enter the land index they want to access, and the owner's name and ID.
3. The program then checks whether the entered owner's name matches the owner name stored for that land in the database.
4. If the entered owner's name matches the stored name, the program prompts the user to enter the document for verification. Then, the program verifies the document's authenticity using the verification() function, which takes the document and other necessary parameters as inputs.
5. If the document is valid, the program proceeds to payment, which is not shown in the code as it is not the goal of the program. The program prints a message indicating that the payment was successful.
6. The user is then asked to enter the new owner's name and ID.
7. The program replaces the old owner's name and ID with the new ones in the document using the hasher() function to generate the old data and replaces it in the document.
8. The program also generates a new signature for the modified document using the signature() function, which takes the document and other necessary parameters as inputs.
9. Finally, the program updates the land data in the database with the new owner name and signature.
10. If the document is invalid, the program prints a message indicating that the document is invalid and that a modification has occurred.

Exchange Block Diagram



1. It first prints the available lands in the database, which is land1 and land2.
2. The user is prompted to enter the index of the first land they want to access (1 for land 1 and similarly for other lands), followed by the owner name and ID for the first land.
3. Then, the user is prompted to enter the index of the second land they want to access, followed by the owner name and ID for the second land.
4. If the entered owner names and IDs match with the owners of the corresponding lands in the database, then the function proceeds with the transaction.
5. The user is prompted to enter the documents for the first land, and the verification() function is called to check if the documents are valid using the digital signature scheme.
6. Similarly, the user is prompted to enter the documents for the second land, and the verification() function is called to check if the documents are valid.
7. If both documents are valid, then the function proceeds with the exchange process.
8. First, the ownership details of the lands are updated in the documents.
9. The updated documents are then saved for future use.
10. The digital signature of the updated documents is generated using the signature() function, and the ownership details of the corresponding lands in the database are updated.
11. Finally, the exchange is deemed successful and a message is displayed.
12. If one or both of the documents are invalid, then a message is displayed accordingly. If the entered owner names and IDs do not match with the owners of the corresponding lands in the database, then a message is displayed accordingly.

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 in order 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 File input, 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 runs over the linear search having complexity $O(n)$.

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

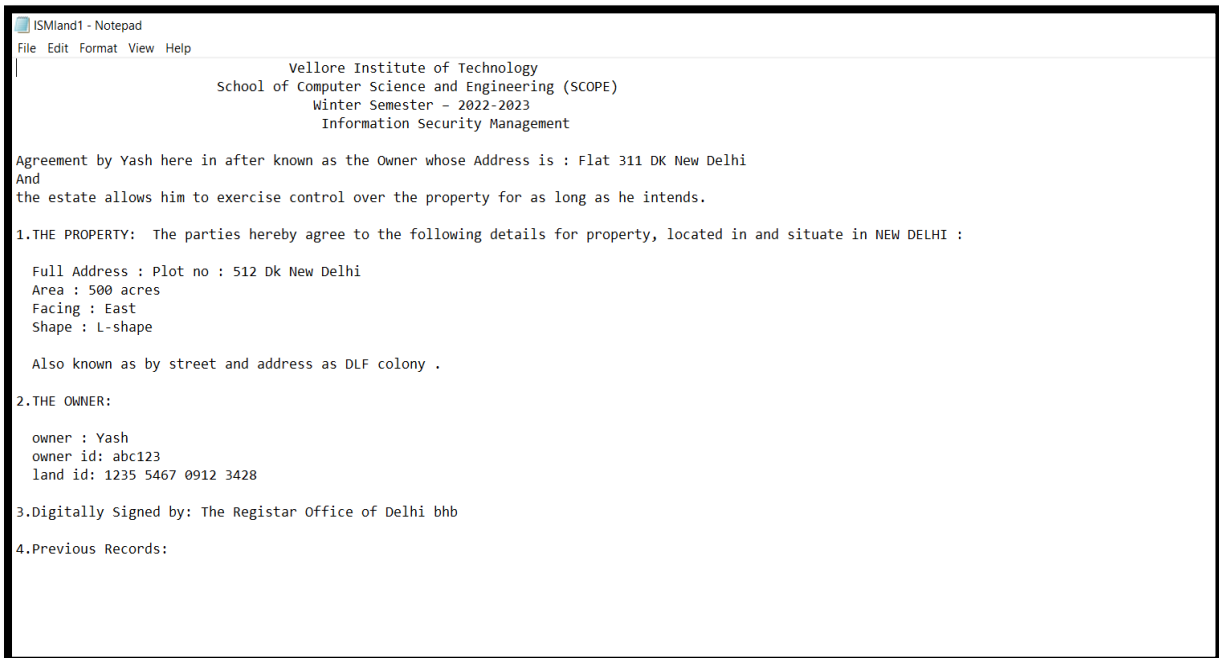
A list of land in the database will appear out of which the two interests are to be selected. After selection the program will ask for the current owner name and the owner id of both the lands in sequence.

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.

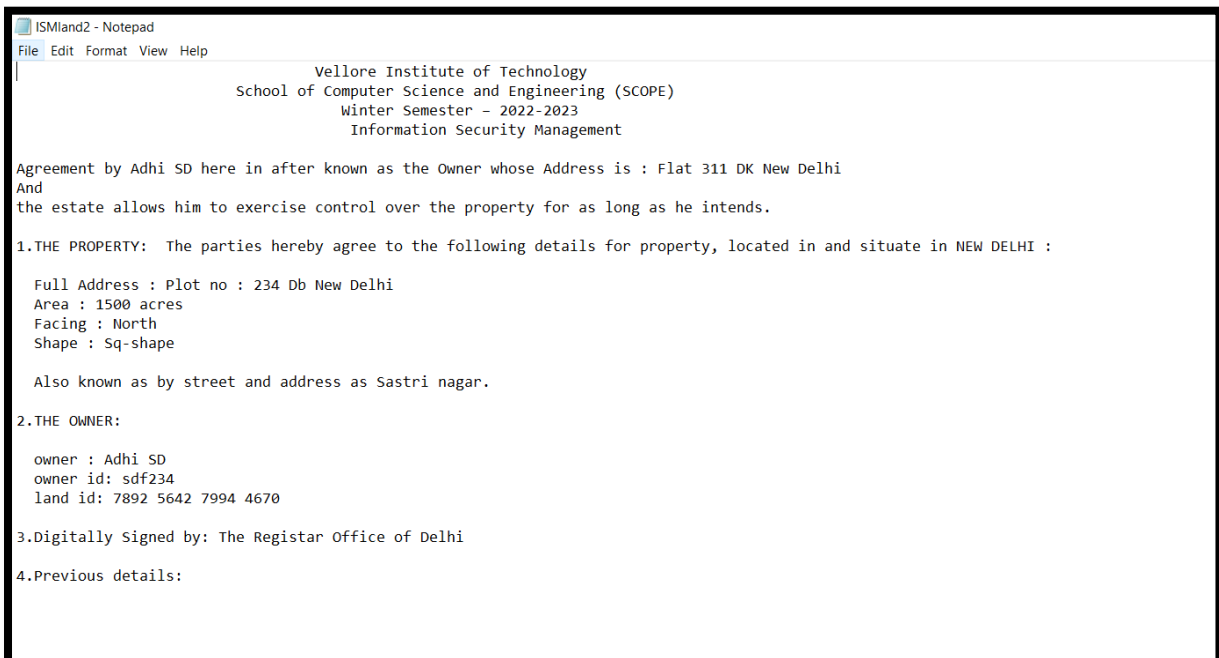
Case3: Exit

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.

Land Document 1



Land Document 2



These are the two Land documents available in the buffer as of now.

It is a menu driven process, so we can see the menu here:

```
****MENU****

1.Transaction
2.Exchange
3.exit

Enter your choice: |
```

There are 3 choices available one is for the transaction of land, one is for exchange of land and the last one is exit.

First we see the results obtained for the transaction.

```
Enter your choice: 1
in database: land1 land2

enter the land you want to access (1 for land 1 and similarly):1

enter owner name: Yash

enter owner id: abc123

enter the documents: C:\Users\Adhithya\Desktop\ISMLand1.txt
the document is valid
the transaction is verified, proceed with payment

payment sucessful

enter the new owner name: Jeevaa

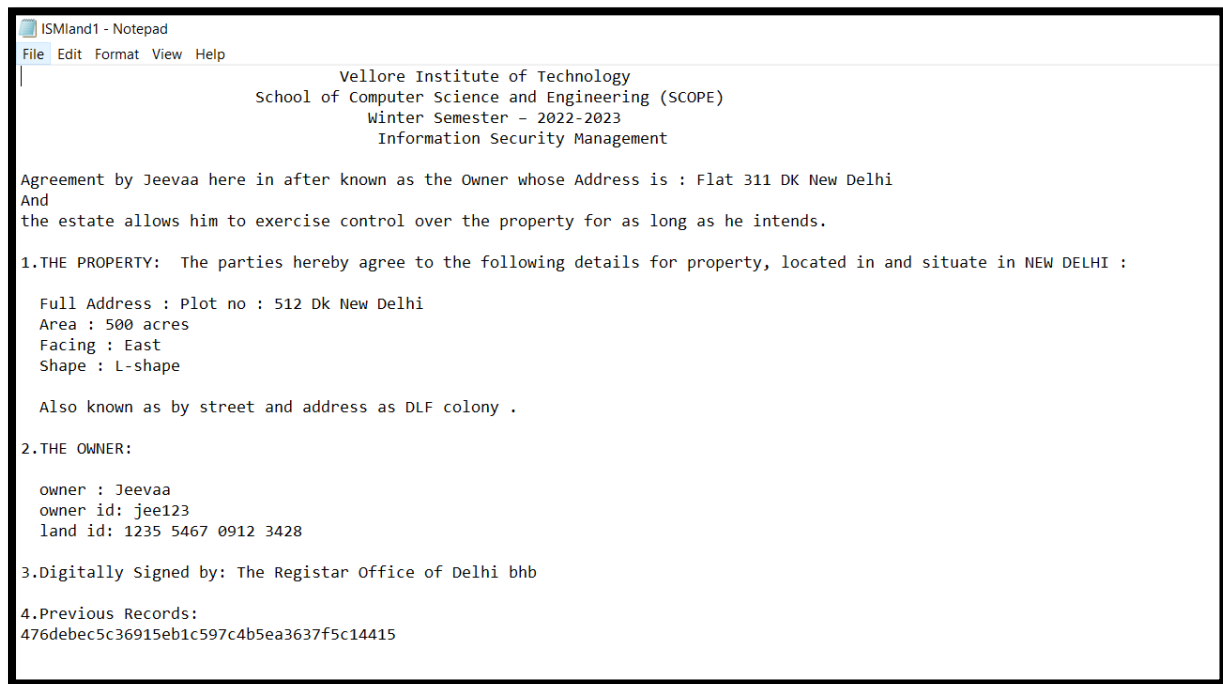
enter new owner id: jee123
the document is modified for future use
the data base is updated

****MENU****

1.Transaction
2.Exchange
3.exit

Enter your choice: 3
Thanks
```

We can see that the land document is updated with the new owner.



```
ISMLand1 - Notepad
File Edit Format View Help

Vellore Institute of Technology
School of Computer Science and Engineering (SCOPE)
Winter Semester - 2022-2023
Information Security Management

Agreement by Jeevaa here in after known as the Owner whose Address is : Flat 311 DK New Delhi
And
the estate allows him to exercise control over the property for as long as he intends.

1.THE PROPERTY: The parties hereby agree to the following details for property, located in and situate in NEW DELHI :

Full Address : Plot no : 512 Dk New Delhi
Area : 500 acres
Facing : East
Shape : L-shape

Also known as by street and address as DLF colony .

2.THE OWNER:

owner : Jeevaa
owner id: jee123
land id: 1235 5467 0912 3428

3.Digitally Signed by: The Registrar Office of Delhi bhh

4.Previous Records:
476debec5c36915eb1c597c4b5ea3637f5c14415
```

It asks for the old owner name and owner id first and verifies it first, then it asks for the land document, once the land document is entered it verifies the document using the digital signature algorithm.

After verification if the document is valid then the transaction is verified and it will allow the user to proceed with the payment.

Once the payment is successful it asks for a new owner name and owner id, after these details are entered the database will be updated. The land transaction has been successfully done.

If some modifications occurred in the document then we get this following results

```
Enter your choice: 1
in database: land1 land2

enter the land you want to access (1 for land 1 and similarly):1

enter owner name: Yash

enter owner id: jee123

enter the documents: C:\Users\Adhithya\Desktop\ISMLand1.txt
invalid document, modification occurred.
```

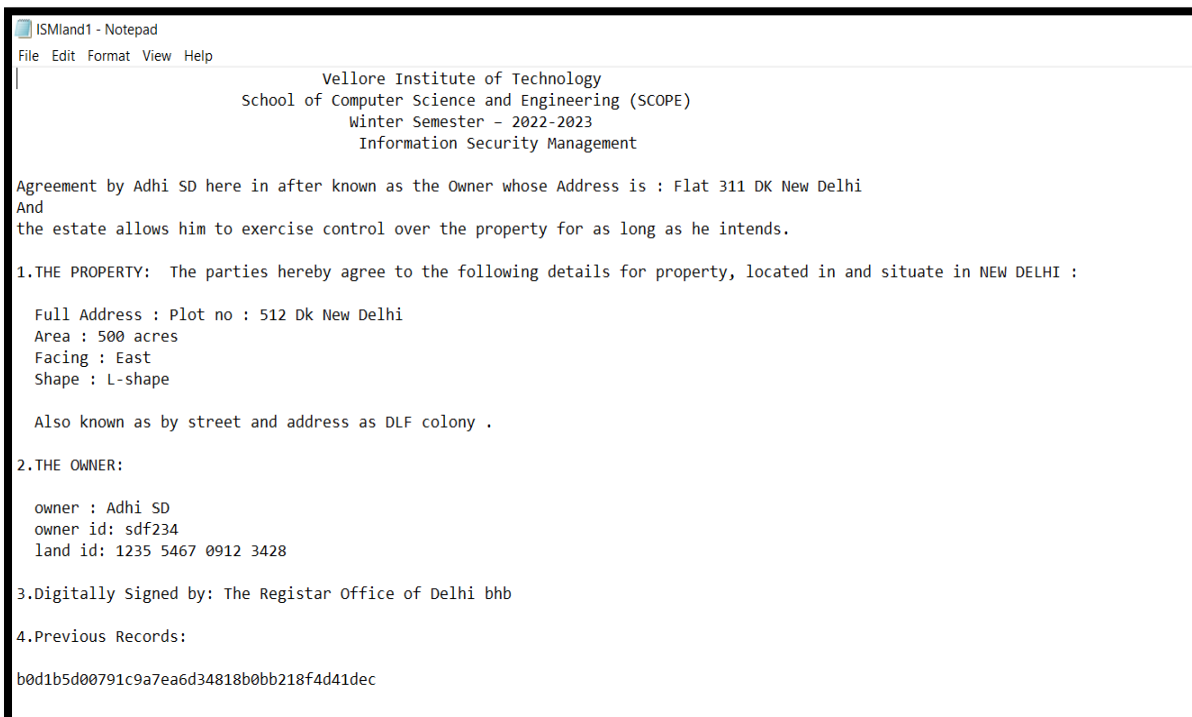
Now we see the results obtained for exchange:

```
Enter your choice: 2
in database: land1 land2

enter the first land you want to access (1 for land 1 and similarly):1
enter owner name for first land: Jeevaa
enter the owner id for first land: jee123

enter the second land you want to access (1 for land 1 and similarly):2
enter owner name for second land: Adhi SD
enter the owner id for second land: sdf234
enter the documents for first land: C:\Users\Adhithya\Desktop\ISMland1.txt
enter the documents for second land: C:\Users\Adhithya\Desktop\ISMland2.txt
the documents are valid and verified
proceed with exchange
document of first land is updated
document of second land is updated
documents updated for future use
first land database udated
second land database updated
exchange sucessful
```

We can see that the land documents have been modified.



ISMland1 - Notepad

File Edit Format View Help

Vellore Institute of Technology
School of Computer Science and Engineering (SCOPE)
Winter Semester - 2022-2023
Information Security Management

Agreement by Adhi SD here in after known as the Owner whose Address is : Flat 311 DK New Delhi
And
the estate allows him to exercise control over the property for as long as he intends.

1.THE PROPERTY: The parties hereby agree to the following details for property, located in and situate in NEW DELHI :

Full Address : Plot no : 512 Dk New Delhi
Area : 500 acres
Facing : East
Shape : L-shape

Also known as by street and address as DLF colony .

2.THE OWNER:

owner : Adhi SD
owner id: sdf234
land id: 1235 5467 0912 3428

3.Digitally Signed by: The Registrar Office of Delhi bbb

4.Previous Records:

b0d1b5d00791c9a7ea6d34818b0bb218f4d41dec

```
ISMLand2 - Notepad
File Edit Format View Help

Vellore Institute of Technology
School of Computer Science and Engineering (SCOPE)
Winter Semester - 2022-2023
Information Security Management

Agreement by Jeevaa here in after known as the Owner whose Address is : Flat 311 DK New Delhi
And
the estate allows him to exercise control over the property for as long as he intends.

1.THE PROPERTY: The parties hereby agree to the following details for property, located in and situate in NEW DELHI :

Full Address : Plot no : 234 Db New Delhi
Area : 1500 acres
Facing : North
Shape : Sq-shape

Also known as by street and address as Sastri nagar.

2.THE OWNER:

owner : Jeevaa
owner id: jee123
land id: 7892 5642 7994 4670

3.Digitally Signed by: The Registrar Office of Delhi

4.Previous details:

a516efdb0ea7a261477e0e7f5d1672f5af17474e
```

Here again it asks for the owner details of the two lands that are to be exchanged, it first verifies the owner details, then it asks for the respective land documents, once the documents have been entered the Digital signature algorithm verifies the documents. Once the documents are verified then the exchange of the lands will be successful.

It will also show if any modifications occurred in any of the documents. This is the obtained result for any modifications in any of those documents.

```
****MENU****
1.Transaction
2.Exchange
3.exit

Enter your choice: 2
in database: land1 land2

enter the first land you want to access (1 for land 1 and similarly):1
enter owner name for first land: Jeevaa
enter the owner id for first land: jee123

enter the second land you want to access (1 for land 1 and similarly):2
enter owner name for second land: Adhi SD
enter the owner id for second land: sdf234
enter the documents for first land: C:\Users\Adhithya\Desktop\ISMLand1.txt
enter the documents for second land: C:\Users\Adhithya\Desktop\ISMLand2.txt
documnet of second land is modified
```

REFERENCE

Mehibel, N., & Hamadouche, M. H. (2020). A new enhancement of elliptic curve digital signature algorithm. *Journal of Discrete Mathematical Sciences and Cryptography*, 23(3), 743-757.

Turn, R., & Ware, W. H. (1976). Privacy and security issues in information systems. *IEEE Transactions on Computers*, 25(12), 1353-1361.

Tawalbeh, L. A. A., & Sweidan, S. (2010). Hardware design and implementation of ElGamal public-key cryptography algorithm. *Information Security Journal: A Global Perspective*, 19(5), 243-252.

Sekhar, M. R. (2004). Signature scheme with message recovery and its application. *International Journal of Computer Mathematics*, 81(3), 285-289.

Islam, S. H., & Biswas, G. P. (2013). Provably secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography. *International Journal of Computer Mathematics*, 90(11), 2244-2258.

Pagnoni, A., & Visconti, A. (2010). Secure electronic bills of lading: blind counts and digital signatures. *Electronic Commerce Research*, 10, 363-388.

Kiayias, A., & Zhou, H. S. (2009). Hidden identity-based signatures. *IET Information Security*, 3(3), 119-127.

Bulens, P., Standaert, F. X., & Quisquater, J. J. (2010). How to strongly link data and its medium: the paper case. *IET Information Security*, 4(3), 125-136.

Pointcheval, D., & Stern, J. (2000). Security arguments for digital signatures and blind signatures. *Journal of cryptology*, 13, 361-396.

Basu, S. (2004). E-government and developing countries: an overview. *International Review of Law, Computers & Technology*, 18(1), 109-132.

Stallings, W. (2013). Digital signature algorithms. *Cryptologia*, 37(4), 311-327.

He, D., Zhang, Y., Wang, D., & Choo, K. K. R. (2018). Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography. *IEEE Transactions on Dependable and Secure Computing*, 17(5), 1124-1132.

Li, M., Weng, J., Yang, A., Lu, W., Zhang, Y., Hou, L., ... & Deng, R. H. (2018). CrowdBC: A blockchain-based decentralized framework for crowdsourcing. *IEEE Transactions on Parallel and Distributed Systems*, 30(6), 1251-1266.

Fromknecht, C., Velicanu, D., & Yakoubov, S. (2014). A decentralized public key infrastructure with identity retention. *Cryptology ePrint Archive*.