Biometric Based Digital Signature Scheme For Land Registry Verification

R.Sinthujan, S.Senthilkumaran, N.Pranavan, V.Vijitharan, Kavinga Yapa Abeywardena

Department of Information Systems Engineering, Faculty of Computing, Sri Lanka Institute of Information Technology

sinthujan1@outlook.com, skdudeflow@gmail.com, pranavann@gmail.com, velaviji@ymail.com, kavinga.y@sliit.lk

Abstract—One of the most common and frequent problem faced by developing countries like Sri Lanka is the management and administration of land properties due to poor land ownership verification mechanisms exercised by government in the sector of land registry department. This leads to cases like land fraudulent, land encroachment, land misuse and land disuse. This research paper states of a biometric based verification scheme for land property management which guarantees the authenticity of land ownership, integrity of land information, and non-repudiation of land transactions. The goal is to generate biometric based asymmetric keys from a personnel's fingerprint to be used for digitally signing the land registry document and then to verify that signature in a secure way where some of the key procedures must take place within an isolated area like sandbox environment to ensure the security and robustness of the system. Also, there are procedures in place for handling disputes that can be confronted when implementing a land management system with biometric verification procedures. This biometric based verification scheme is not limited only within the boundaries of the land registry domain, but can also be extended and applied as a generic solution for many other similar domains where the verification procedure is vital and a must.

Keywords— Biometric Keys, RSA Algorithm, Digital Signature, Land Registry

I. INTRODUCTION

Land is a crucial component in human lifestyle as land can be considered as one of the most valuable asset of people which have both commercial and financial market values helping in the economic and social development in a country like Sri Lanka [1–4]. Land registration is the process of recording information about the land including the ownership, boundaries, area, location and various other details [2, 3]. However, from the past experiences we can learn that there is a considerable amount of land frauds, land encroachment, misuse and disuse of land took place all around the country [4].

The most common and frequent problems that can be identified within the domain of general public with regard to the land assets due to poor verification procedures are – uncertainty of ownership to a land asset, more than one person or one party claiming for the same piece of land, contradictions between the land documents of different parties with regard to some critical fields like limits of the land, area of the property and location of the asset, selling of a piece of land to an innocent buyer by an impersonator who is not the actual owner by faking the documents, land encroachment and misuse, domination over a piece of land by one party where more than one parties are co-owning the land property, difficulties in proving the ownership to a land property, misuse of state owned lands, and the difficulties in land sales through power of attorney to a land asset [3, 4].

Unfortunately, due to the lack of systematic procedures in handling land registration, absence of proper and consistent communication between stakeholders, growth of political motivated and economic motivated land mafias – the land registration system of the country is subjected to a large scale of land problems. The main reason for these land related issues is that there is still no proper and sophisticated verification procedures and methodologies implemented in the domain of land registry management [1]. Therefore, the research on "Biometric based digital signature scheme for land registry verification" is aimed to add more features and functionality to the existing land registry management by implementing biometric based authentication and verification.

II. LITERATURE REVIEW

A. Sandbox

Sandbox is a secure mechanism to test untested codes to make sure that will not affect the entire system which will limit the internal functions and restricted unnecessary access by giving enough access to allow proper actions while not exposing the critical systems to potentially flawed code [5, 6]. Sandbox will provide an isolated and dedicated environment to test, understand and take action on the threats [7].

B. Ron Rivest, Adi Shamir and Leonard Adleman (RSA) Algorithm

RSA is an asymmetric key algorithm that supports both encryption and digital signature procedures. This algorithm uses intractability of integer factorization problem which provides security to this algorithm and therefore is the most widely used public key algorithm. RSA uses two different keys namely the private key and public key having a mathematical relationship to each other [8]. The algorithm's security relies on the assumption that having access to one key won't help to figure out the other key and on the fact that it is easier to multiply two large prime number together and get a resulting product, but you can't guess the two original prime numbers from the product value itself [9].

C. Key Generation in RSA

i. Choose two distinct large prime numbers p and q

ii. Calculate n = p*q

- n is used as the modulus for both the public and private keys.

iii. Compute ϕ (n) = (p-1)*(q-1)

- This value is kept private

iv. Choose an integer e such that $1 < e < \phi(n)$ and gcd $(e, \phi(n)) = 1$; [e and $\phi(n)$ are co-prime]
- e is the public key exponent

v. Determine d as $d \equiv e{-}1 \pmod{\phi(n)}$; [d is the modular multiplicative inverse of e (modulo $\phi(n)$)]
- d is the private key exponent

vi. Public key consists of modulus n and the public exponent e

vii. Private key consists of modulus n and the private exponent d

D. Biometric Cryptosystems

The domains of cryptography and biometrics are combined and integrated together to form a powerful new technique called biometric cryptosystems to provide the advantages of each of the two domains for security purposes. This helps the biometric cryptosystem to provide with superior and modifiable security levels, which are considered as the advantages of cryptography domain and getting rid of the need to know/memorize passwords or carry tokens and uniqueness of the biometric traits of the person, which are the advantages of using biometrics.

E. Biometric Key Generation

Generation of cryptographic keys using the fingerprint as the biometric feature uses the fingerprint image to extract the minutiae points from the ridges where the minutiae points set are used for generating of the keys to be used in cryptosystems. This is the process of converting live biometric data into a key(s) of bit-string representation.

F. Digital Signature and Verification

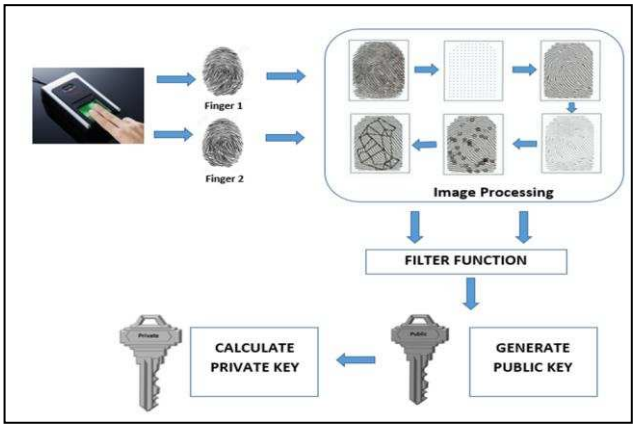
Digital signatures are strong mechanisms applied in order to achieve the security services of authentication (proof of identity of the sender), data integrity (detection of changes to the message) and non-repudiation (prevention of denial of sending the information) [10].

Message => M; Signature => S;
Public Key => {e, n}; Private Key => {d, n};

Signing => $S = M^d \bmod n$
Verification => $M' = S^e \bmod n$; if $M' \equiv M \bmod n$, then signature is valid

III. METHODOLOGY

A. Asymmetric Key Generation using Biometrics



Fingerprint Acquisition

The land owner's biometric identities are acquired from two different fingers using a dedicated fingerprint reader and the raw data is passed in to the system for further processing [8, 12, 13].

Image Processing

The received fingerprint images are processed using specific image processing algorithms and the original fingerprint is subjected to go through different phases such as setting the orientation, image enhancement, image binarization, thinning of fingerprint, minutiae point extraction and finally feature representation [8, 9, 11, 13].

Both of these received fingerprints should go through this image processing function separately and the final outcome is stored as inputs for the filter function, where the final outcome of each fingerprint is represented as two different value sets of bit-strings.

Filter Function with Sophisticated Algorithms

Now both fingerprints have different two bit-string values associated with them which are derived from their extracted biometric identities, and now these values are subjected to go through a filter function designed using sophisticated algorithms to make sure that these values are formatted in a way to support in the key generation procedure to be used in asymmetric encryption algorithms (here RSA) for the sole purpose of digital signature and verification techniques.

The filter function is to be designed in a way to reproduce the exact same formatted values each time the same biometric identities are inputted in to the system – thus, this filtering function plays a prominent role in the key generation process and is considered as the heart of the proposed system's functionality.

Generation of Public Key and Calculation of Corresponding Private Key Using RSA Algorithm

After going through the filter function, both the fingerprints will have formatted values ready to be applied in the key generation process that are associated with RSA Algorithm.

The large prime number "n" is calculated by multiplying prime numbers "p" and "q" where both "p" and "q" are the values derived from the first fingerprint template.

The public exponent "e" is generated using the values derived from the second fingerprint template and is adjusted in a way that it is smaller than and co-prime to the Euler Phi function of n [$\Phi(n)$].

Then, the private exponent "d" is calculated such that this private exponent is the multiplicative inverse of public exponent "e".

B. Key Handling & Key Storage

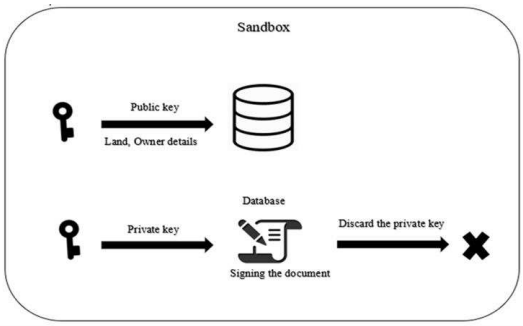
Key management is as predominant as key generation. All the keys generated in the system are going to be managed in this phase. Initially the land owner(s) should register their details and land details to the system therefore key pair should be extracted from his/her biometric (fingerprint) by the previous process. Here in this process, public key from the key pair is going to be saved in the database with relevant land, land owner(s) details and the private key will be transferred through the current process to

next process for digital signature. Once the signing procedure is finished, the private key will be discarded immediately in a secure manner. Implementation of this step will be helpful for later verification process.

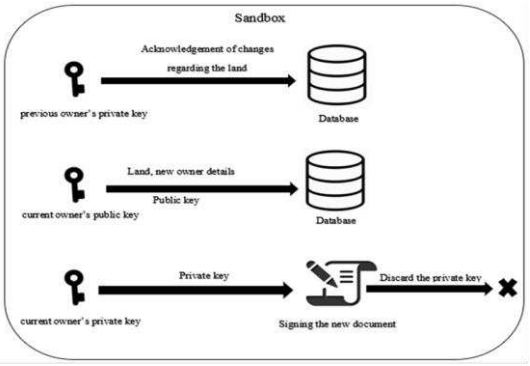
The changes in land property ownership during land transfers / changes in power of attorney cases will be considered as a different scenario that will need a different approach. Land owner's private key will be taken to verify his acknowledgement regarding land related or ownership changes. Then the buyer or the new owner's private key and public key will be taken, and public key is saved in the database with the relevant land and ownership details, where the private key will be taken for signing the new document and after that procedure the private key will be securely discarded.

All these procedures should be done in a secure manner. The system should ensure that all the private keys generated within the system should not be compromised or exploited by unauthorized parties during the key generation and signing processes, but the handling of public keys doesn't need to be bothered much. Therefore, a sandbox environment is going to be used for these processes which will limit the internal functionalities and restrict some of the system's actions to make sure the entire system can handle the biometric keys generation and temporary storage facilities without leaking the sensitive data to the outside environment. The isolated environment will help to make sure that the biometric key related processes are handled in a secure way. The biometric key at the fly will be protected by different approaches and after the signing process using private keys, these private keys and other biometric information will be discarded within the sandbox environment in a way that they are not recoverable at any instance.

Initial Land Registration



Land Transfer



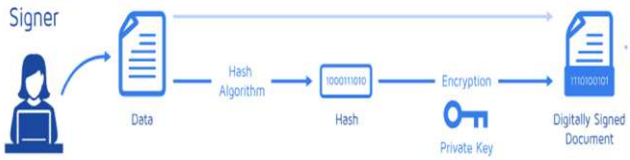
The sandbox environment is created by Sandboxie software and key discarding and key protection mechanism is implemented inside the system.

C. Digital Signing & Verification

Digitally Signing the Land Document

Step 1: - A hash value of the land document is calculated by applying cryptographic SHA3 hashing algorithm.

Step 2: - Digitally signing a document, the information obtained in the first step – the hash value of the document is encrypted with the private key of the land owner(s) who sign the document and therefore the encrypted hash value (signature) is obtained. For this purpose, cryptographic RSA encrypting algorithm is used.

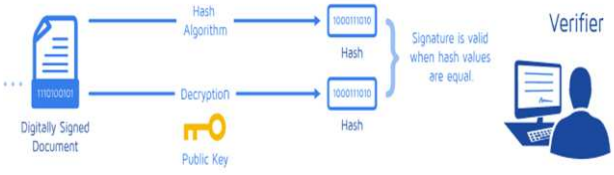


Verifying the Digital Signature of a Land Document

Step 1: - A hash value of the presented document is calculated. For this calculation, the same hashing algorithm is used that was used during the signing process which is SHA3 hashing algorithm. The obtained hash value is called as the current hash value because it is calculated from the current state of the document.

Step 2: - The digital signature verification process, the digital signature is decrypted with the same RSA encryption algorithm that was used during the signing process. The decryption is done by the public key that corresponds to the private key used during the signing of the document. As a result, we obtain the original hash value that was calculated from the original document during the first step of the signing process.

Step 3: - Compare the current hash value obtained in the first step with the original hash value obtained in the second step. If the two values are same, the verification of the digital signature is considered successful and hence proves that the current state of the document is exactly same as the state of the original document which is signed with the private key of the land owner(s) during the registration phase. If those two values differ from each other, then it means that the verification is unsuccessful and there has been some modifications in the current document when comparing to the original document's state/content during signing process at the registration phase.



D. Event Log Management

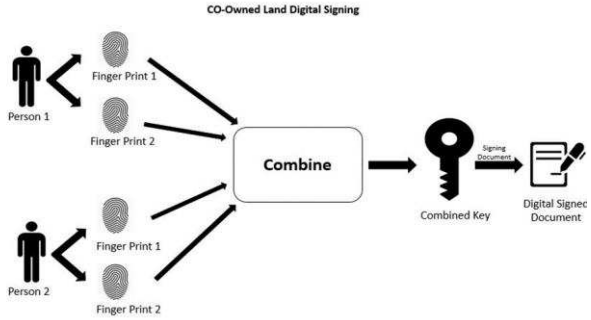
Event Viewer allows to display actions in system. It maintains logs about modification, activities and system events on the computer system. It uses Event Viewer to view and manage the event logs, collect information about actions made by users. The Event Log service starts automatically, when the system starts. An authorized user can view an application and system logs. Logs are save as read only format, so that no one can edit the log file. This will help to maintain the integrity and non- reputation of the system.

E. Dispute Resolution

Dispute resolution of Biometric Based Digital Signature Scheme for Land Registry Verification has sub-parts in order to give various solution to various issues.

In a situation of Proving the efficiency, integrity and trustworthy of the system, we must provide explanations related to the complaints and should be able to illustrate the ambiguity of the implemented scheme with a help of transparent dummy system where all important progress (input, process, output) of the system are transparent to the users. This system will be used in closed environment, because if it is landed in the wrong hands - it may break the security of the system.

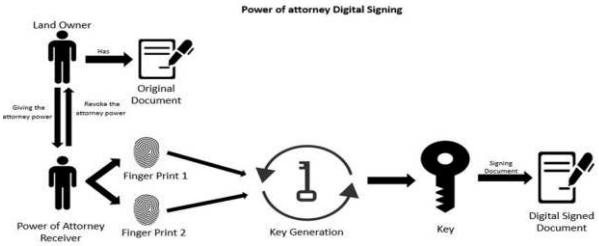
Co-owned land is the one which has more than one owner. In that case, fingerprints will be taken from the owners (two different fingerprints from each owners) and by combining them the key will be generated and that key will be used to sign the document. When they plan to sell their land, presence of all owners of the land is must in order to sell the land.



When registering a land to a company/organization (not to a particular person). In this case, fingerprints will be taken from the CEO or Management Members of the organization and the keys will be generated - then the private key will be used to sign the document. In the document it will be mentioned that the land is belonged to the organization, and not to the particular persons. So, when the management changes they can provide the legal documents, revoke the old signature and sign it with new keys.

State owned lands - those lands owned by the government will be signed using the biometrics of corresponding government officials and are marked as government property because state-owned lands cannot be sold by individuals. Digitally signing these state owned lands reduce conflicts and forgeries when it comes to verification phase.

Giving power of attorney to someone - apart from the original document, there will be another digital document created and signed by the receiver. In the document the conditions will be mentioned. And the original owner of the land can revoke the power of attorney at any time he/she wants.



Defining the conditions and the responsibilities of the system – implementation of an information security policy stating what kind of actions are allowed by the system, what kind of actions can't be tolerated by the system and what are the responsibilities of system users. This will be helpful to take legal action when the user breaks the rules.

IV. RESULTS & DISCUSSIONS

In real time implementation of our system, SecuGen Hamster Plus device is used for acquiring the fingerprints of the users and Sandboxie software is used for implementing the sandbox environment.

Using the fingerprint images acquired from the fingerprint reader, the minutiae points are extracted using an algorithm developed in Java which incorporates some major components from an open source algorithm SourceAFIS – after being introduced to the filtering function which does some alterations to the original minutiae coordinates, these minutiae point coordinates are used to calculate the asymmetric keys which are then used to digitally sign and verify the land registry documents as per their use cases mentioned in the methodology section.

In Sandboxie software, restrictions and resource access are tested with sample programs - specifically internet, network and file access. This worked as expected and because of its light weight manner, its performance is 40% higher than the other sandboxes.

V. CONCLUSION & FUTURE DIMENSIONS

The proposed solution is aimed to implement biometric based digital signature scheme for land registry verification, which guarantees the authenticity of land ownership, integrity of land information, and non-repudiation of land transactions. Generation of exactly same asymmetric key value pairs in all of the instances for a specific biometric set of user(s) is ensured by the biometric based asymmetric key generation. The system related risks

regarding private keys are eliminated by runtime protection and safe key discarding techniques implemented using sandboxing technique. The functionality of the system differs in accordance with the type of land ownership, and the future works are handled by dispute resolution. The outcome of this research is an efficient and effective solution for land registry verification using biometric based digital signature scheme.

For the future works, further researches can be done in the biometric based verification scheme to extend the knowledge gained from the above research, and apply them as a generic solution for many other similar domains having the verification procedure(s) as a must in their functionalities.

ACKNOWLEDGEMENT

First, we would like to thank Sri Lanka Institute of Information Technology, for providing the opportunity and platform to develop and expose our skills and abilities via performing a research project and for all collective arrangements done to make this module successful. This project would not have been possible without the guidance of our research supervisor Mr. Kavinga Yapa Abeywardena. We would like to sincerely thank him for the valuable insights and supported us to make this a success. His guidance and concern provided throughout the research of our project is thoroughly appreciated. Our collective thinking, effort and collaboration is what made our project a success.

REFERENCES

[1] J. Jayakody, "An analysis of land ownership rights in document registration: A pragmatic Sri Lankan perspective", Repository.kln.ac.lk, 2018. [Online]. Available: http://repository.kln.ac.lk/handle/123456789/7765. [Accessed: 01- Apr- 2018].

[2] Kirubananthan, "Evaluating Land Governance Issues in Land Titling Programme (A Case Study in Sri Lanka)", Webapps.itc.utwente.nl, 2018. [Online]. Available: https://webapps.itc.utwente.nl/librarywww/papers_2013/msc/la/kirubananthan.pdf. [Accessed: 01- Apr- 2018].

[3] T. Perera, "Implementing Land Registration Systems in Sri Lanka: Being Pragmatic", 2018. [Online]. Available: http://journals.sjp.ac.lk/index.php/SLJRE/article/download/114/48. [Accessed: 01- Apr- 2018].

[4] H. Buddhisena, "Registration of Titles to Land - An new approach ", Island.lk, 2018. [Online]. Available: http://www.island.lk/2002/03/15/featur02.html. [Accessed: 01- Apr- 2018].

[5] P. Craig, "What is a sandbox? And why do I need one to defend against advanced threats?", Sophos News, 2018. [Online]. Available: https://news.sophos.com/en-us/2016/04/13/what-is-a-sandbox-and-why-do-i-need-one-to-defend-against-advanced-threats/. [Accessed: 01- Apr- 2018].

[6] "Sandboxes Explained: How They're Already Protecting You and How to Sandbox Any Program", Howtogeek.com, 2018. [Online]. Available: https://www.howtogeek.com/169139/sandboxes-explained-how-theyre-already-protecting-you-and-how-to-sandbox-any-program/. [Accessed: 01- Apr- 2018].

[7] "What is a Sandbox (in Computer Security)? - Definition from Techopedia", Techopedia.com, 2018. [Online]. Available: https://www.techopedia.com/definition/27682/sandbox-computer-security. [Accessed: 01- Apr- 2018].

[8] M. T. Rashid and H. A. Zaki, "RSA Cryptographic Key Generation Using Fingerprint Minutiae," Iraqi Comm. Comput. Informatics ,Iraqi J. Comput. Informatics, vol. 1, no. 1, pp. 66–69, 2014.

[9] V. Conti, S. Vitabile, and F. Sorbello, "Fingerprint traits and RSA algorithm fusion technique," Proc. - 2012 6th Int. Conf. Complex, Intelligent, Softw. Intensive Syst. CISIS 2012, pp. 351–356, 2012.

[10] D. Mann, S. Gupta, A. Sharma, and S. Akhtar, "Digital Signature using Biometrics," vol. I, no. 2, pp. 6–7, 2015.

[11] R. Ranjan and S. K. Singh, "Improved and innovative key generation algorithms for biometric cryptosystems," Proc. 2013 3rd IEEE Int. Adv. Comput. Conf. IACC 2013, no. i, pp. 943–946, 2013.

[12] P. Balakumar and R. Venkatesan, "Secure Biometric Key Generation Scheme for Cryptography using Combined Biometric Features of Fingerprint and Iris," IJCSI Int. J. Comput. Sci. Issues, vol. 8, no. 5, pp. 349–356, 2011.

[13] "Minutiae Based Extraction in Fingerprint Recognition", Bayometric, 2018. [Online]. Available: https://www.bayometric.com/minutiae-based-extraction-fingerprint-recognition/. [Accessed: 01- Apr- 2018].

[14] L. You, G. Zhang, and F. Zhang, "A fingerprint and threshold scheme-based key generation method," Proceeding - 5th Int. Conf. Comput. Sci. Converg. Inf. Technol. ICCIT 2010, pp. 615–619, 2010.

[15] Make Tech Easier. (2018). 6 of the Best Sandbox Applications for Windows 10 - Make Tech Easier. [online] Available at: https://www.maketecheasier.com/best-sandbox-applications-windows10/ [Accessed 15 May 2018].

[16] Developer.apple.com. (2018). About App Sandbox. [online] Available at: https://developer.apple.com/library/content/documentation/Security/Conceptual/AppSandboxDesignGuide/AboutAppSandbox/AboutAppSandbox.html [Accessed 15 May 2018].

[17] Risto Vaarandi. Platform Independent Event Correlation Tool for Network Management. Proceedings of the 8th IEEE/IFIP Network Operations and Management Symposium, pp. 907-910, [2002].

[18] NIST, "National institute of standards and technology [docket no: 070911510-7512-01]announcing request for candidate algorithm nominations for a new cryptographic hash algorithm (SHA-3) family," Federal Register, November 2007.

[19] J. P. Aumasson, L. Henzen, W. Meier, and R. C. W. Phan, „SHA-3 proposal BLAKEversion 1.3," NIST SHA-3 Competition.

[20] P. Gauravaram, L. R. Knudsen, K. Matusiewicz, F. Mendel, C. Rechberger, M. Schlffer,and S. S. Thomsen, "SHA-3 proposal grostel version 2.0.1," NIST SHA-3 Competition.

[21] Professor N. Selvakkumaran, University of Colombo, Tiernan Mennen, Abt Associates, "Land disputes and development in Sri Lanka implications of the vestiges of crown land", February 24, 2017.

[22] Zakout, W, Wehrmann, B, Torhonen, “Good Governance in Land Administration. Principles and Good Practices”, 2007.
[23] Alden Wily, Liz, “Whose Land Is It? Commons and Conflict States. Why the Ownership of the Commons Matters in Making and Keeping Peace”, 2008.
[24] Gershin Feder, “The Benefits of Land registration and titling economic and social perspectives, Land Use Policy”, 1999.