TEST Engineering & Management

*March - April 2020*
*ISSN: 0193-4120 Page No. 2137 - 2143*

# Secured Identity System

Amartya Mathew, Vishwakarma Institute of Technology, Pune, India, amartya.mathew17@vit.edu
Chinmay Kulkarni, Vishwakarma Institute of Technology, Pune, India, chinmay.kulkarni17@vit.edu
Yash Kulkarni, Pune Institute of Computer Technology, Pune, India, yashkulkarni99@gmail.com

***Article Info***
***Volume 83***
***Page Number: 2137 - 2143***
***Publication Issue:***
***March - April 2020***

***Article History***
***Article Received****: 24 July 2019*
***Revised****: 12 September 2019*
***Accepted****: 15 February 2020*
***Publication****: 18 March 2020*

***Abstract:***

A proof of concept of a novel secured electronic identity system where every valid citizen of a country will have a key pair with which they can prove their identity. This system will also not allow fake identities to be created easily.

***Keywords:*** *Certificate Authority Hierarchy, Asymmetric Key Encryption, Symmetric Key Encryption, Hashing, Digital Signature, Certificate Authority (CA), Secure Hashing Algorithm (SHA), Rivest, Shamir and Adelman (RSA)*

## I. INTRODUCTION

We often depend upon trust a lot of time in our day to day lives. When someone claims to be who they are they we could ask them to submit documents in to prove it. The problem is that a document be it a hard or soft copy can easily be faked. Our proof of concept eliminates this need to trust people and provides a system where anyone can verify claims of this nature. The proof of concept uses the following to achieve this task:

1) Asymmetric Key Encryption
2) Symmetric Key Encryption
3) Hashing
4) Digital Signature
5) Certificate Authority Hierarchy

## II. THEORY

### *A. Encryption*

Encryption can be thought of as a transformation of readable text into text that seems to have no meaning at a glance. Decryption is the exact opposite of encryption. To perform encryption and decryption something called a key. In a sense, the key can be thought of as something that locks or unlocks a message as and when required.

It is almost impossible to figure out a message that has been encrypted by modern-day algorithms. In symmetric-key encryption, the same key used to lock the message is used to unlock it. In our case, however, we need to use asymmetric key encryption as it can also be used as a digital signature.

In asymmetric key encryption, we use a key pair which is a pair of keys generated at the same time. If a message is locked or encrypted by one of these keys only the other key can unlock or decrypt it. It is not feasible to guess the other key given one of the keys from the key pair. From the key pair, one of the keys is referred to as a public key (intended to be known by all) and the other is called a private key (intended to be known only to the owner of the key pair).

For our implementation, we have used AES and RSA encryption schemes. Brute force attacks against these algorithms are practically impossible. The current best attack on AES-128 takes 2^126.1 operations, if we had a computer (or cluster) several million times more efficient than any current computer and could operate at the thermodynamic Landauer limit, it would take 234 petajoules just to increment a counter through every key value.[7]

March - April 2020
ISSN: 0193-4120 Page No. 2137 - 2143

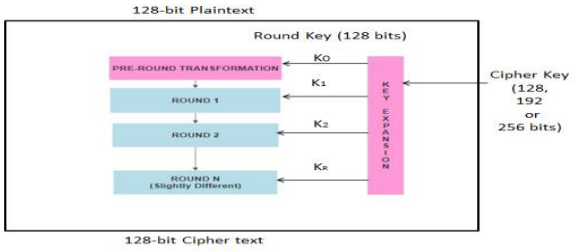


Fig 1: Block Diagram of AES Algorithm

The security of RSA comes from the computational difficulty of factoring large numbers. The factors of the public key n, that is, p and q should be large enough so that it is not easy to factorize n. So, large prime numbers should be used. In general, the order of the primes should be 160 (512 bits) digits to 640 (2048 bits) digits. No algorithm is available that could factorize a number of the mentioned order in a reasonable amount of time. One has to use brute-force to factorize n. The algorithms to factorize n have a running time exponential with respect to the length of n. Still, the existence of a faster algorithm, to factorize n, is very remote. So the RSA algorithm is defended by the non-availability of such algorithms.[6]

Consider X and Y who wish to communicate in secret. X writes the message and encrypts or locks it with Y's public key (X can easily obtain Y's public key as Y will broadcast it). After this when Y wishes to read the message Y simply uses the correct private key to decrypt or unlock the message. To reply Y encrypts the message with X's key and the process continues.

*B. Hashing*

Hashing is the use of a mathematical function to map data of arbitrary size to a certain value of a fixed size. Hashing can essentially be thought of as a fingerprint of a given string.

Hashing is used in cybersecurity to make sure that messages are not tampered with. A cryptographically secure hashing algorithm must have the following properties:

1) The length of the output is fixed irrespective of the length of the input.
2) It is impossible to predict the input string given only a hash value.
3) Each input string has a unique hash value. Even a small change in the input string will give a completely different hash value.
4) For a given input string the output hash value will always be the same

We will use a member of the Secure Hashing Algorithm family called SHA-256. The 256 refers to the length of the output string in bits.

*C. Digital Signature*

A unique property of asymmetric key encryption is that if the message is locked with one of the keys only the other key can unlock the message. This can be used to act like a signature used in our day to day lives. We had discussed the example of X and Y. If a message is encrypted by X private key the only thing that can unlock it will be X's public key.

This seems counter-intuitive to security but this can be used to prove that only X could have written the message (this is assuming only X knows the correct private key). This is the principle behind a digital signature where a message is first hashed, and then the hash is encrypted with a private key. A receiver of the message can decrypt the hash with the correct public key. Then the receiver can hash the message received. If the hashes are the same then it can be confirmed that the message was sent by a certain person and was not tampered with.[2]

*D. Certificate Authority Hierarchy*

A vulnerability of asymmetric key encryption is that it is susceptible to man in the middle attacks. Assume X wishes to communicate with Y so X broadcasts a request for Y's key.

However, if a malicious third party (Z) intercepts this message then Z can send his/her public key to X.

Z would then send the message to Y and Y would respond with the intended public key. So X and Y communicate without knowing Z is reading and/or modifying their messages. This why when X sends a request for a public key, X must also request a certificate signed by an authority certifying that the given public key does indeed belong to Y. [1]

However, we need a way to verify that the signature is from a valid authority. To solve this issue a Certificate Authority Hierarchy is created. There is a root Certificate Authority which signs the certificates of the people working right under him/her. The officers under the root CA are called the second level CA who signs the certificate of the third level CA. This structure relieves the pressure of the root CA who does not have to sign every user's certificate. The root CA's public key is treated as public knowledge. Using this anyone participate in a network can check if the certificate is valid or not.

*E. Document Forgery*

Forging of documents has existed as long as documents themselves. There are 3 ways to forge documents:

1) Steal a legitimate document
2) Bribe an official
3) Apply for a document with a false name

A well-funded adversary would be able to steal everything that a person uses as a unique identifier including documents and/or biometric data.

Comprehensive reference manuals and databases for highly protected security documents, particularly banknotes, passports, and visas, try to keep updated collections of images from authentic documents, including close-up views and specifications of relevant security features.

Also, document experts of immigration and forensic science services are networking information on detected counterfeits and forgeries. This is a valuable help for fast authenticity checking, mainly at the front line of inspection. For many other documents, however, this type of reference material does not exist. This would mean criminals could forge documents that don't have this kind of security like birth certificates or mark-sheets and use those documents to apply for the more secure documents under false names. The current system also fails to account for the fact that an official with enough right to an identity database could easily issue false documents and leave no evidence of this.

Most of the times security personal do not have the equipment to conduct an in-depth check for the document. Documents are also not necessarily always submitted to only security personal. There are situations where documents can be submitted to vendors also who would almost certainly not have any sort of training to spot forged documents.

## III. WORKFLOW

*A. Registration*

The citizen must approach a government office to be registered. The citizen can generate a key-pair if desired however; this is not required as a key pair can be generated by the officer at the office. At the office, a citizen must present valid documents to prove their identity. Then the citizen must enter their public key and complete a small challenge to prove they have the corresponding private key. After this, the citizen is to present a DNA sample and fingerprint data. The DNA sample will never be visible to anyone. It will be processed internally.
The DNA is used to prove that an applicant is unique and human.

It is also to prevent someone from registering twice. We will not directly store the DNA samples but will hash the samples then encrypt and store them. This adds an extra layer of security to protect this critical data.

March - April 2020
ISSN: 0193-4120 Page No. 2137 - 2143

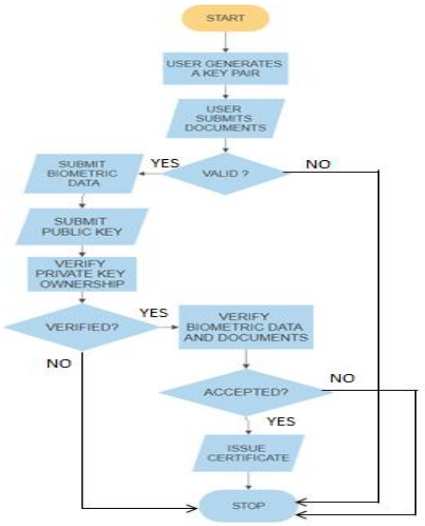


Fig 2: Flowchart of Registration Process

Unfortunately, we cannot do the same for fingerprints. Fingerprints will be stored as they are captured as we will not be able to compare the hashes of fingerprints. However, they will be encrypted. Fingerprints are used to provide another layer of authentication when someone is trying to use a key pair. The last bit of biometric data to be collected is a photo of the person's face.

If the citizen has submitted valid documents, has provided valid and unique biometric data and has a unique key pair then the officer can issue a certificate for the citizen. For government officers also there will be registration like this done where they will be verified by their superiors. The most superior government entities' public key will be treated as public knowledge. This is where the principle of Certificate Authority Hierarchy will allow anyone to verify the details of others.

*B. Storing Keys*

All officers' public keys are made available to the public. Now officers will retire or get transferred due to which old key pairs must be discarded for security reasons. This, however, can create a lot of problems as a list of key pairs changed or transferred must be maintained.

To avoid this issue in our implementation the private key of a key pair will not be known to anyone even the officer who has the key pair. The private key will be stored in an encrypted file. The key for this file can be changed every time the key pair is to be handed over to a new officer.

To use the private key the officer simply has to enter the password for the encrypted file and give the correct fingerprints and the program will load the private key for use for a fixed time.

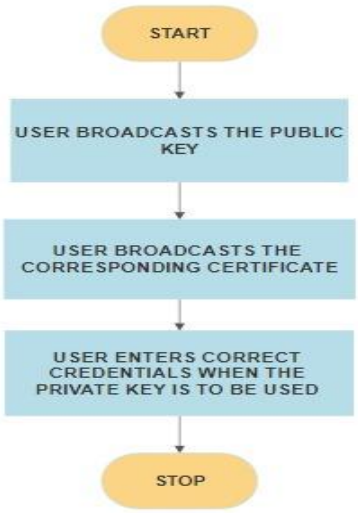


Fig 3: Usage of key pair

Citizens are encouraged to encrypt their key pair immediately after generation to avoid theft of the keys. Citizens are also instructed never to share their private key as it can be used to impersonate them. Citizens' private keys will also be stored in files that are encrypted and require biometric data and a password to access. They also will be temporarily being loaded into the computer for use.

*C. Usage of the key pair as a document*

When a person wishes to prove their identity all they need to do is to submit their public key and its certificate. Every member of the public in a given country will have their country's certificate authority hierarchy available to them. Hence they can use this information to ensure that the certificate was indeed signed by a valid entity of the government. Since the

signature of the certificate is valid we can easily say that the key pair is not tampered with.

Now to prove that the person is a legitimate owner of the private key once simply has to encrypt a message and send it the person whose identity is to be verified. If the person can decrypt the message this means that they have the private key file and the data required to unlock it.

A more secure way of doing this is to exchange a key and ask the receiver to send a message that is encrypted with the said key.

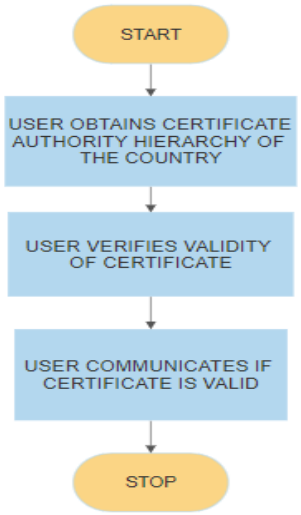


Fig 4: Using someone else's certificate

*D. Forgery Technique Mitigations*

Our new technique prevents all but the well-funded adversaries to be able to steal the document. Stealing biometric data, the private key and reduplicating a face is something only the well-funded entities will be capable of. If citizens are alert then it would become all the more difficult to steal the documents.

Government officials trying to add false entries
A corrupt government official would have to add completely new biometric data which is not easy to do. There are certain tools available that allow people to generate new biometric samples of data. However, the official would also have to present some other documents to validate the identity of the person. The documents in questions could be issued by another entity in a different organization which would mean there is someone else who would also have to be involved. Even if the official is successful in getting forged biometric data and documents the certificate for the new document must still be signed by the officer with a digital certificate that can easily be used to prove the officer's misdeeds. If all organizations were to follow the scheme we have suggested any members of the public community can easily verify the legitimacy of a given document due to the certificate authority hierarchy.

If for example, someone tries to apply for a passport under a false name this person has to obtain a falsified certificate. Anyone who would issue a certificate would have to also sign the same and this could easily be traced back to them. Hence there will be very few people willing to do this. Since the person is unable to obtain a false certificate it would not allow them to obtain other falsified documents.

*E. Trusting Documents Obtained From Different Countries*

Now there could be a problem when a person from country A visits country B. Country B's security personal wish to know if this person from country A has falsified their document or not. Another problem is when a person from country A is in country B, someone could try to trick them into believing they hold a certain position in the government and could use this to trick the visitor from country A. After all, the entire visitor does not have the certificate authority hierarchy of that country. Now the certificate authority hierarchy of a given country can be made available even to citizen of another country but this does not solve the problem as a person from another country has no reason to trust the certificate authority hierarchy of another country so to solve this problem the root certificate of a country must be signed by the root certificates of other countries. This would allow for international verification of identities.

March - April 2020
ISSN: 0193-4120 Page No. 2137 - 2143

## IV. Alternative Applications

### A. Usage In Agreements

When parties draft a document with all terms and conditions it shall be signed by all of them in a given order.

Suppose P1 P2 and P3 come on a business agreement and draft a contract. They will also have to specify the order in which they signed the contract. All this data is put into a hashing algorithm and the hash is first signed with the private key of P1. Next P2 signs the hash and then P3 concludes the process.

If one of them violates the terms of the contracts the other two can easily prove that the third party had signed the contract using the following method.

So P2 and P3 can once again hash the contract which gives a hash H1.

Now they take the signed hash and decrypt it with their public keys. The hash will be signed only by P1's public key. Next, thy use P1's key and decrypt the hash H2. Now they can show that H1 is equal to H2. Since the use of the private key also requires the use of biometric information it can be concluded that P1 did sign the contract.

### B. Pre-Shared Key

Although asymmetric cryptography algorithms are relatively easier to understand and implement they are much slower than symmetric cryptography algorithms.

To gain speed security and convenience we can easily use a combination of symmetric and asymmetric cryptography. To have a secure communication system two parties must agree on a pre-shared symmetric key. Every time two parties need to communicate one of them can generate a symmetric key.

The symmetric key will be encrypted by the public key of the receiver. Once the receiver decrypts the message both parties will use the same pre-shared key. Now the transmitter can encrypt and send it.
The receiver can easily ask for proof also to make sure that the transmitter is the legitimate owner of the key.

### C. Secure Sharing Of Documents

Assume that someone wants to securely share a document. The document will be hashed and signed by the owner. Then the document will be encrypted by pre-shared key and then will be sent securely.

### D. Proof of Position Of Assets

This system can also be used to eliminate the need for paper documents where numerous problems exist. In our system, these documents will be online and will have the signature of valid government officers. A system where total assets values can easily be calculated allows for better taxation as well. This system can also be used to record bank transactions above a fixed amount to ensure money is not being used for illegal purposes.

### E. Employee Certificate

This may sound similar to the secure sharing of documents but a certificate to prove that a person is in a position at a certain organization requires more complexity.

We could try to keep one public key for one organization. However, this means that each employee will have some sort of access to the key. Giving the key to only one person would be very inconvenient for others. Instead, all organizations must have an internal certificate hierarchy. The root certificate of this organization can be signed by a member of parliament. Now when someone wants to verify that they are communicating with a valid

person of a valid organization, they can use the same process of validating a citizen's identity.

### *F. Eliminating Passwords*

Instead of using passwords important accounts can be secured by security tokens that can be sent to the holder of the key pair. Doing this process completes KYC quickly and adds all the security of the key pairs to the online account. If a person wants to log in for online banking, a token can be encrypted and sent to the user. The user will need access to the corresponding private key which means the user needs the password to the private key and biometric data making it harder for malicious parties.

## V. Future Scope

Our implementation uses the RSA algorithm for asymmetric encryption. RSA requires keys of large size and computationally expensive. RSA is also based on factoring of large primes and better algorithms are being made for factoring numbers though they are still exponential. This puts the security of RSA at risk. We wish to use Elliptic Curve Cryptography so we can reduce key sizes and provide more security.

## VI. Conclusion

This new identity system will enable more security for individual identities. This system will also allow for better taxation of non-salaried people. This system also reduces the trust individuals need to place on each other. It also allows people to communicate securely and share important documents in a secure manner where all details can easily be verified.

## VII. References

[1] Atul Kahate, “Cryptography and Network Security”.
[2] William Stallings “Cryptography and Network Security Principles and Practice”.
[3] Menezes, Van Oorschot and Vanstone “The Hand book of Applied Cryptography”.
[4] http://ravindraranwala.blogspot.com/2019/05/rsa-cryptosystem-proofs-of-correctness.html?m=1.
[5] https://doi.org/10.1063/1.3526259.
[6] https://crypto.stackexchange.com/questions/2884/rsa-proof-of-correctness/2894.
[7] https://www.eetimes.com/how-secure-is-aes-against-brute-force-attacks/.
[8] https://crypto.stackexchange.com/questions/24307/why-is-aes-unbreakable.
[9] https://www.atpinc.com/blog/what-is-aes-256-encryption.
https://criminal.findlaw.com/criminal-charges/forgery.html.
[10] https://www.comparitech.com/blog/information-security/what-is-aes-encryption/.