[1]Prof. Rakesh Bhavsar,

[2]Dr. Madhavi Dave,

[3]Dr. Pooja Shah,

[4]Hetal A. Joshiyara,

[5]Chintan Patel

Enhancing Data Security in Banking: The Power of Hybrid Algorithm-Based Solutions

Abstract: - A safe financial system requires a safe security system. It takes a secure banking system to stop sensitive data from being stolen from customers and banks. Important information may be quickly and easily exchanged online in the modern society. A hacker may more easily take our information the easier it is to transmit information. Thus, a robust security mechanism is necessary. Currently, a banking system must guarantee the secrecy of the customer's data in order to preserve the customer's trust in the system and data security. Bank-based security systems are made secure by means of cryptographic methods.

In RSA and ECC, two keys are generated: a private key and a public key. It is the best data security technique to protect the bank against online fraud. Stated differently, the digital signature standard and associated message verification are created by both public key algorithms. Moreover, the Diffie Hellman algorithm is calculated to provide the user's keys in a secure way. Regarding mutual authentication and key exchange, it is evident that ECC is more robust and offers more advantages than RSA. Elliptic Curve Cryptography and Random Access Keys (RSA) are two distinct asymmetric algorithms that are used in this research to create a strong security system that improves data security and takes into account key exchange and mutual authentication between two untrusted parties. Our system is protected against unwanted access by the use of the encryption methods RSA and ECC.

Keywords: Banking system security, RSA, Cryptographic methods, ECC, Data security

I. INTRODUCTION

In our day-to-day lives, network security is crucial. Due to the pandemic, online learning and living have become commonplace in our lives, making it crucial to safeguard the environment, integrity, and confidentiality from attackers who are always looking for and taking advantage of holes in systems that are already in place. Faults can occur in devices, data, applications, users, and places. Data security is the process of preventing unauthorized access to and corruption of data throughout its lifespan [1]. Data security solutions provider Micro Focus has over 80 patents and 51 years of experience. Micro Focus's big data solutions make even the most difficult use cases easier to understand. Robust data encryption, tokenization, and key management to safeguard information across apps, transactions, storage, and big data platforms in a more straightforward and secure manner. Protecting against malicious attacks on computers, servers, mobile devices, electronic systems, networks, and data is known as cyber security.

It is often referred to as electronic information security or information technology security. The phrase can be broken down into numerous categories and is used in a wide range of applications, including business and mobile computing. All the security breaches lead to hacking, ransom ware, password attacks, malware, blackmailing, and middle-man attacks, among others. The threats, problems, online surveys, and future consequences of social networking are all extensively discussed in this study. A Safe Banking system requires a strong security system these days as there are many incidences of hacking occurring A secure banking system is necessary to prevent and safe case the essential information of the bank and client from getting hacked. In recent times, the maximum amount of information flow is occurring through the medium called the internet and the transaction is occurring fast and easy. Exchanging our information is frequent, and the easier the

[1]PhD Scholar, Indrashil University, Kadi, Gujarat, India, Email: rakesh.bhavsar08@gmail.com

[2]Project Manager - IoT Security, DIASVPCoE, Gujarat University, Gujarat, India

[3]Associate Professor, IT Department, VSITR,Kadi Sarva Vishwavidyalaya, Gujarat, India. Email:poojaz.2608@gmail.com

[4]Assistant Professor, Computer Engineering Department, L. D. College of Engineering, Ahmedabad,Gujarat, India. Email:hetaljoshiyara@gmail.com

[5]Academic Associate, Ravi J Matthai Centre of Educational Innovation, Indian Institute of Management, Ahmedabad,Gujart, India. Email:chintanp@iima.ac.in

hacker is to steal our information to gain his motive. It is still the same situation even in the security system of the bank. So, a strong and impenetrable security system is needed and accessibility of computer networks and data in its most basic form. Every business, regardless of size, sector, or infrastructure, need network security solutions to defend itself from today's ever- increasing spectrum of cyber threats. The network architecture of today is complex, and it must fight with an ever-changing threat everywhere these days. In present times, the confidence of client on the banking system is especially important, so ensuring security client's data is necessary and should also maintain confidentiality and authenticity. To ensure security for bank-based security system cryptographic techniques are used. The cryptography techniques which are used in this project are

RSA algorithm and ECC algorithm with inputs both text and image type. There are two types of cryptography algorithms which are well known that are symmetric cryptography and asymmetric cryptography algorithms. The symmetric cryptography algorithm operates it is both encryption and decryption process with the same key. The asymmetric cryptography algorithm operations require different key for encryption and different key for decryption. So, it is more secure when compared to symmetric cryptography algorithm. Both RSA and ECC Algorithms which are used in this project are examples of asymmetric cryptography algorithm. The examples of symmetric cryptography algorithm are DES, 3DES, AES, bow fish techniques and more. The examples of asymmetriccryptography algorithm are RSA, ECC, Diffie Hellman algorithms. The ECC algorithm is more than RSA algorithm because ECC consists of Diffie Hellman algorithm where shared keys are present which increases security than RSA Algorithm.

Fig-1. Goals of Cryptography

II. LITERATURE SURVEY

These days, a safe financial system requires a strong security system in particular. A secure banking system is necessary to prevent hackers from gaining access to sensitive bank and consumer data. In this current day, sharing of critical information, files via the internet are exceptionally rapid and simple these days. The quicker trade of our information has gotten, the easier the hacker is stealing our information to obtain his purpose. If banking systems are included, the situation is identical. So, a good security system is necessary everywhere currently, data security and client data confidentiality are crucial for maintaining client trust in the financial system. To ensure security for bank- based security system cryptographic algorithms are used. There are two main types of cryptography algorithms which are symmetric and asymmetric key cryptography, in this project, asymmetric key cryptography is used, in which RSA and ECC algorithms are compared in different ways or components to know which algorithm is better. In RSA Algorithm, two prime numbers are used to follow up the process of the algorithm but in the ECC Algorithm, any two points in the elliptical curse are used to continue with the process. The same key is used by the symmetric cryptography technique for both encryption and decryption. Asymmetric cryptography algorithms require distinct keys for encryption and decoding. As a result, it is more secure than symmetric cryptography algorithms. Asymmetric cryptography algorithms include the RSA and ECC algorithms, which are used in this project. DES, 3DES, AES, bow fish methods, and other symmetric cryptography algorithms are examples. The RSA, ECC, and Diffie Hellman algorithms are examples of asymmetric cryptographyalgorithms. The ECC algorithm is more secure than the RSAalgorithm because it includes the Diffie Hellman algorithm, which uses shared keys to boost security. [2]

Digital Signature:

Nowadays there is a use of digital data everywhere. Digital data can be stored, transported copied, and

modified easily. So, there is a problem of unauthorized access and stealing data when using digital data. These security problems can be solved using a digital signature. Digital Signature is like an attachment to a digital document or a fingerprint that provides authenticity and integrity. Signatures are sent along with messages as a separate document when the document is signed digitally he receiver receives both message and signature when the message is digitally signed. By using the message and signature, the receiver checks for the authenticity of the message. A digital signature prevents the data from unauthorized access.

Key Factors of Digital Signature:

There are mainly four key factors of Digital Signature. They are:

Privacy/ Confidentiality: Privacy refers to the protection of data from unauthorized access and modification. It means that a third-party intruder can't see or change the data sent betweentwo people.

Authentication: Authentication serves as evidence that the data is being accessed by the authorized user and not by an unauthorized third party. Authentication is necessary for establishing trust between parties. To prevent data from being modified, authentication is also required when a user logs into the network.

Integrity: It refers to the ability to prevent unauthorized access to data, messages, or transmissions. By prohibiting unauthorized access to the data and undesirable alterations, data integrity is protected. External and internal consistency, as well as other attributes like completeness, accuracy, and so on, can all be ensured through integrity. [3]

Non-Repudiation: The assurance that the other person cannot deny that they sent the messages known as nonrepudiation. This protects the communication from being intercepted by an unauthorized party. As a result, when the receiver receives the message, he can prove that he is the one who sent it.

In a digital signature, the sender adds a unique code to the message that serves as a signature. The signature is created by taking the message's hash value and encrypting it with the sender's private key. The message's integrity is ensured by the signature. The sender sends the receiver the signed and encrypted message. The receiver receives the signed and encrypted message and uses the same hash function to check whether the message was received correctly or if theunauthorized user made any changes.

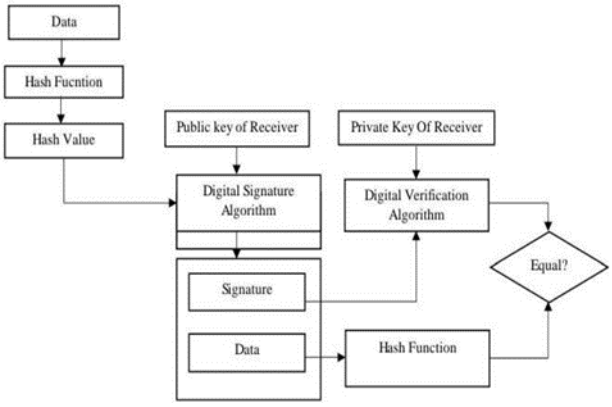

Figure 2: Block diagram of Digital Signature

III.SYSTEM DESIGN

RSA and Digital Signature using MATLAB

RSA algorithm is the basic algorithm used for security purposes. The essential steps followed in the RSA algorithm are Key Generation, Key Distribution, Encryption, andDecryption.

The equation for the encryption is P'=En*(PUBr, P)the equation for the decryption is P=De*(PRIr, P')

RSA Algorithm is on the steps of key generation, encryption, and decryption and Q are 2 prime numbers and Ø (n) is calculated.

n= p*q

Ø (n) = (p-1) *(q-1)

Then, the private key (d) and public key (e) are produced, withthe private key being derived from the formula =>d*e*mod

(n) =1 and the public key being generated at random in the range of 1e (n).Perform encryption by using these public and private keys to form the cipher text from the given plain text. To verify the algorithm, decryption is performed to get the plain text from the cipher text.

Operations of RSA Algorithm key Generation

In RSA, the equations required for encryption and decryptionin the exponential form are:

P'= $P^{(e)}$ *mod n is the equation for Encryption ofthe Publickey (e, n)

P= $P'^{(d)}$ *mod n is the equation for Decryption of the Privatekey (d, n)

- Choose any two prime numbers between and q.
- Now solve for n=p * q.
- Substitute (n) for (p(*q) = (p) *(q) =(p-1) * (q-1) (If 'a' is aprime number, (a)Equals (a-1).)
- Choose 'e' such that 1 = e (n) and 'e' is likewise the co-prime to 'n' (n).

Now'd' value can be determined by using the formulae:e*d = 1* mod Ø (n)

Because 'e' and (n) are co-prime integers,'d' will be themultiplicative inverse of 'e' in this instance. The followingformulas were used to compute the value of'd':D=(Ø(n)i+1)/e

Encryption

The encryption of a communication starts when the private and public keys have been produced. Plain text is alwaysencrypted in blocks using RSA. Each plain text block should have a binary value of n. The public key of the receiver is employed in the encryption process. The expression to compute the cypher text is as follow:

P'= $P^{(e)}$ *mod n

Decryption

Following the encryption process, the RSA decryption processstarts, this needs a cypher text and the private key of the matching public key used in the encryption phase. The expression to compute the plain text is as follow: P= $P'^{(d)}$ *mod n

Confidentiality and Authentication which are the two mainproblems of the symmetric key cryptography can be overcome by using the double public keycryptography.

RSA Digital Signature

Digital signature is used to strengthen the security of the RSA algorithm. If only RSA is used, there won't be enough security to prevent unauthorized users from accessing the system.. When the digital signature is used with the RSA algorithm,the security of the algorithm gets increases. By combining both digital signature and the RSA algorithm more integrity is also obtained, authentication, and non-repudiation. It becomes hard for unauthorized people to access the data that is transmitted using digital signature and RSA algorithm. In RSA-DS Algorithm, compare the Hash function of the received message and the decrypted message to check whether it satisfies the digital signature or not, first encryption and decryption of the message is done to ensure the security of the data or message and then pass it through the code of the digital signature to verify if digital signature is satisfied or not.

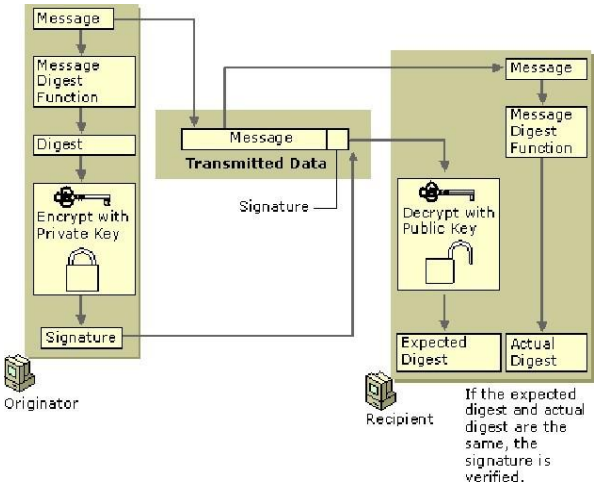

Figure 3: RSA algorithm using digital signature Input as text:

For the case of giving input as text, the text is given in the command window which is presentin the mat lab software when the code is being run. For this case of giving input as an image, the image file is saved in the same file as that code's mat lab file is saved to get them in the same sourceand the image name is mentioned in the code itself to facilitategetting the output faster when the code is run.

RSA – IMAGE

Encryption and decryption of the data which is present in the form of both text and images is used to analyze the performance of the algorithm. In RSA-IMAGE Algorithm,the input given is in the form of image and to give the image asan input, image is needed to be saved in the existing file in which code is saved in the mat lab file and the remaining process is the same as the one where text is needed to be givenas input. To compare the two algorithms RSA and ECC, time taken is a criterion used for the completion of operation and time taken for the key generation and security. To know the time, A function called tic and toc is used which are used inthe start and end of the code [4].

Diffie Hellman Algorithm using MATLAB: Diffie Hellman Algorithm is present in the ECC algorithm. So first the Diffie Hellman algorithm is executed, and the output is obtained. In a Diffie Hellman algorithm, the sender and receiver will get the same key which is called the common key or secret key after the algorithm is executed.

In the Elliptic Curve Cryptography algorithm, the Diffie Hellman key exchange algorithm is used for secure communication between two users.

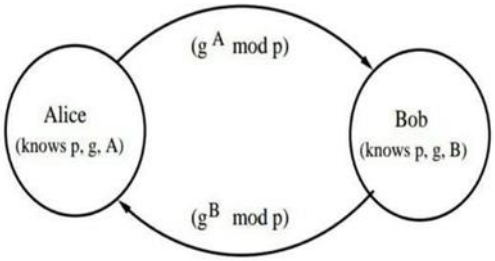

Figure 4: Working of Diffie Hellman Key Exchange Algorithm

Diffie-Hellman Key Exchange Algorithm:

In the subject of Cryptography, the Diffie-Hellman techniqueis one of the early instances of key exchange. The Diffie-Hellman algorithm appeared by Diffie and Hellman in 1976.The Diffie-Hellman method enables the two persons do nothave any information about each other, to jointly construct asecret shared key via an unsecured communication channel.The Diffie-Hellman algorithm comes under asymmetriccryptography, and it is used to establish a shared secret for asymmetric-key algorithm. Many protocols use this algorithm [3]. For example, SSL, Secure Shell, and IPSec use this algorithm. In the Diffie-Hellman algorithm, the two parties

agree on oneshared key and then the secured communication channel isestablished between them. In this algorithm, in this method,the two parties need to have public or private key pairs. Thesender uses a private key, while the recipient uses a public key. Both the keys are calculated together, and the shared key is created. Now this shared key is utilized by both sender andrecipient. The shared key is used as a shared symmetric cryptographic key or to produce a content-encryption key. The fundamental purpose of the Diffie-Hellman method is tosafely exchange the keys and produce the common sessionkeys.

In this algorithm, there are two public numbers shared by the two parties. They are a large prime integer p and g is the primitive root of a.

Let us assume there are two people A and B. A is the sender and B is the receiver.

Let the private key selected by A be Xa and theprivate key selected by B be Xb.

Now calculate the public key of A, Ya with thefollowing equation Ya = (g^Xa) mod p

The public key of B is Yb, Yb = (g^Xb) mod p A and Bexchange their public keys.

To calculate the shared keys Ka of A and Kb of B, they usethe public keys that are exchanged. Ka = (Yb^Xa) mod p

Kb = (Ya^Xb) mod p

Ka will be equal to the Kb which is the shared key.

The above picture (figure 4) tells the Structure of the DiffieHellman Key Exchange Algorithm.

Alice and Bob exchange their public keys and generate a secretkey between them [4].

ECC and Digital Signature using MATLAB

The Elliptical curve equation is y^2=x^3+ax+b.The curve is symmetrical to the x-axis.

On the elliptic curve consider two points P (x1, y1) and Q (x2,y2) which are rational. Draw a line through the points P andQ, then the line meets the elliptic curve at the third rational point R [11].

Calculate the prime number p on the elliptic curve E which is given by Y^2= x^3+ax+b (mod p) with a base point P on E User A selects a private key as Ka and user B selects the private keyas Kb.

The public key of user A is Qa=Ka*PThe public key of user Bis Qb=Kb*P

To increase the security of the Elliptic Curve Cryptography algorithm digital signature is also used. By using only ECC, there is not enough security from being accessed by unauthorized users. When the digital signature is used with theECC algorithm, the security of the algorithm gets increases. By combining both digital signature and the Elliptic Curve Cryptography algorithm more integrity, authentication, and non- repudiation are obtained. It becomes hard forunauthorized people to access the data that is transmitted using digital signature and ECC algorithm. By taking each other's public keys, User A and User B calculate the secret key for user A -> K = Ka*Qb For user B -> K=Kb*Qa

For Encryption:

Let the message be M. First encode this message M into a point on the elliptic curve, and namethe point as Pm.

For Encryption choose a random positive integer k.

The cipher point will be Cm= {K*P, Pm+K*Qb} this point will be sent to the receiver. Secure communication between them

For Decryption:

Multiply x-coordinate with the receiver's secret key K*P*Kb

Then subtract (KP*Kb) from the y coordinate of cipher point Pm+K*Qb-(K*P*Kb)

Qb=Kb*P. So therefore Pm+K*Qb-K*Qb

Pm is obtained after decryption. The receiver get the samepoint.

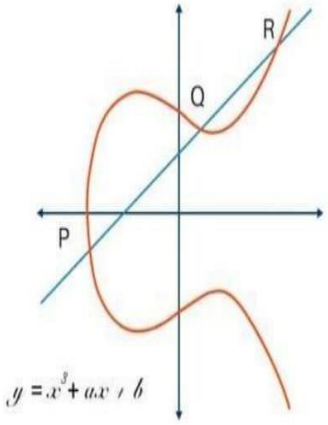

Figure 5: Elliptical curve equation graph [10]

Hybrid Algorithm (RSA and DiffieHellman Algorithm)using MATLAB:

RSA provides less security than ECC. The security of RSA is tried to improve by combining RSA with the Diffie Hellman key exchange algorithm. In the RSA algorithm, the Diffie Hellman key exchange algorithm is used for exchanging the keys between the sender and receiver [5].

First by using the Diffie Hellman key exchange algorithm, thesender and receiver first share their public keys with each otherand compute the common key for both sender and receiver After the sender and receiver share the common key then RSA encryption is performed by the common key at the sender sideand the encrypted information is transmitted to the receiver.Now even if the unauthorized user gets the encryptedmessage, they cannot get the original message from it because only the receiver has the common key to decrypt the message At last, when the encrypted message goes to the

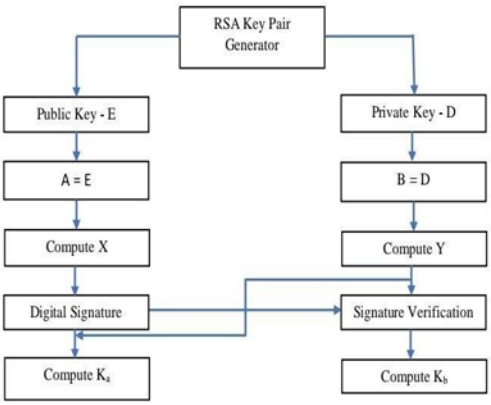

Figure 6: Working of Hybrid Algorithm

Receiver, the message is decrypted using the common keywhich is the same as the sender's common key at the receiver. By doing this the security of the RSA algorithm gets improved. But this process takes more time as first the common keys should be computed between sender and receiver. So, this algorithm cannot be used when an algorithm that takes less time is needed. When security is more important than time, this algorithm can be used. ECC algorithm already has Diffie Hellman key exchange algorithm as part of the algorithm. ECC takes less time than a hybrid algorithm for encryption anddecryption. So Elliptic Curve Cryptography algorithm is preferred over the hybrid algorithm because it takes less time and provides almost the same security [9].

IV. RESULTS AND DISCUSSION

RSA, Digital Signature using MATLAB: The plain text is encrypted and decrypted using RSA and Digital Signature using MATLAB. Digital Signature is verified as the message digest of the transmitted message is

equal to the message digest of the received message. The time taken to complete encryption and decryption using RSA and Digital Signature inMATLAB is 11.227 sec.

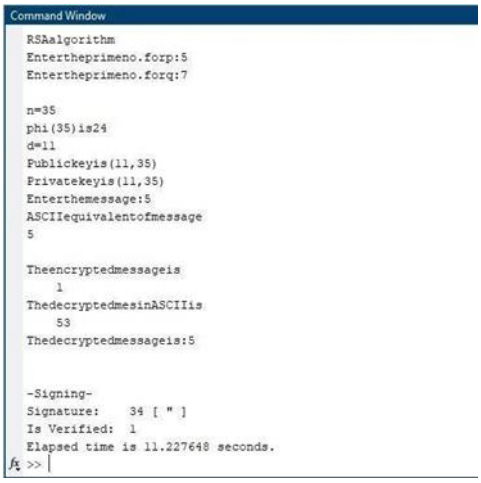

Figure 7: RSA and Digital Signature -Text as input

RSA Image Encryption and Decryption

The fingerprint is taken as an image and is encrypted and decrypted by using the RSA algorithmand Digital Signature inMATLAB [12].

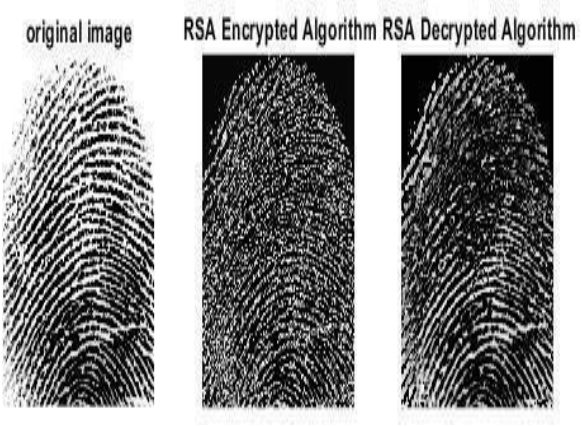

Figure 8: RSA and Digital Signature - Image asinput

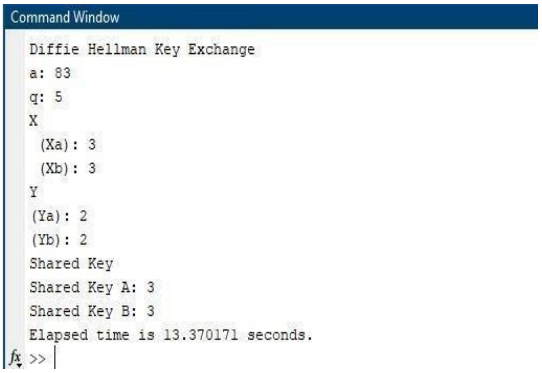

Figure 9: Diffie Hellman Key Exchange Algorithm

Diffie Hellman key exchange algorithm is verified as the shared key is the same for both sender and receiver. Thesender and receiver can use this shared key for a secure transaction between them. The time taken for the Diffie Hellman key exchange algorithm is 13.370 sec.

Elliptical Curve Cryptography and Digital Signature

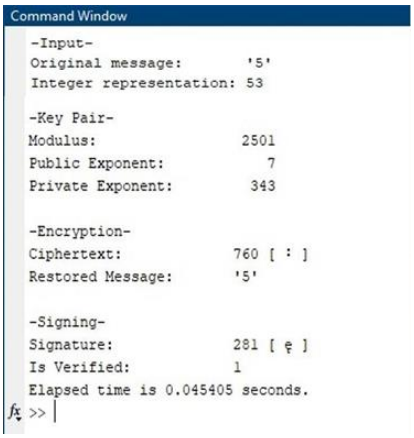

Figure 10: ECC and Digital Signature - Text asinput

ECC Image Encryption

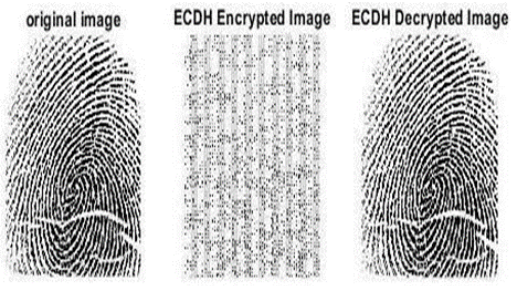

Figure 11: ECC and Digital Signature - Images input

The fingerprint is taken as an image and is encrypted and decrypted by using ECC algorithm and Digital Signature in MATLAB [6,7].

Hybrid (RSA and Diffie Hellman)

The RSA and Diffie Hellman Algorithms are combined toobtain more security. The plain text is encrypted and decrypted using Hybrid algorithm. The time taken to complete encryption and decryption using Hybrid algorithm in MATLAB is 12 sec. The Hybrid algorithm takes more time than ECC. So, Hybrid algorithm cannot be used where encryption and decryption of an algorithm requires less timeto compute. Hence, ECC is preferred over Hybrid algorithm [8].

Figure 12: Hybrid Algorithm

V.CONCLUSION AND FUTURE SCOPE

Conclusions

ECC is more secure than RSA because the key exchange algorithm in ECC shows its authenticity and confidentiality. ECC takes less time for encryption and decryption compared to RSA. Time taken for encryption and decryption of the RSA algorithm is 11.227 sec and ECC algorithm is 0.045 sec. The Key Generation time for Digital Image is less for ECC when compared to RSA. The key generation time for RSA algorithm is 0.654 sec and for ECC algorithm is 0.312 sec. The ECC algorithm takes less time than the Hybrid algorithm. So ECC is better than RSA for a secure bank-based datasecurity system. A hybrid algorithm offers more security than the RSA algorithm.

Future scope

At present, data security must be ensured in every sector.Hacking is constantly becoming increasingly active as hackers are trying to find new ways when the technology is improving. In line with them, the designs and implementations should be made to form an impenetrable strong security system. There is an opportunity to work further with the system because of

network and security. Normalization of finger print usage while online transactions can be considered in the future. Ministries, Large companies, etc. can also use the new security system along with the securebanking system. Face recognition or iris scan is a possible modern technology that can be used to increase the security of the system.

REFERENCES

[1] Ali, S., Abdullah, T. P. T. A., Athar, A., Hussain, A., Ali, M., Yaseen, M., Joo, M. I., & Kim, H. C. (2023). Metaverse in Healthcare Integrated with Explainable AI and Blockchain: Enabling Immersiveness, Ensuring Trust, and Providing Patient Data Security. Sensors (Basel, Switzerland), 23.

[2] Pavan kumar S.Aruna Deepti, E.Sreenivasa Rao (2022). Comparison of RSA and ECC Public key cryptography techniques in WSN". Journal of VLSI Design tools&Technology vol 12 issue 1

[3] Islam, Md & Kobita, Aysha & Hossen, Md & Rumi, Laila& Karim, Rafat & Tabassum, Tasfia. (2021). Data Security System for A Bank Based on Two DifferentAsymmetric Algorithms Cryptography. 10.1007/978-981-15-5258-8_77.

[4] Tara Salman, Student Member, IEEE, Maede Zolanvari, Student Mem-ber, IEEE, Aiman Erbad, Member, IEEE, Raj Jain, Fellow, IEEE, and Mohammed Samaka, Member, IEEE "Security Services Using Block- chains: A State of the Art Survey" IEEE CommunicationsSurveys & Tu-torials (Volume: 21 , Issue: 1)

[5] Sankalp Jagga and Puneet Sharma (2014). Banking Authentication Technique" International Journal of Information & Computation Technology. ISSN 0974- 2239 Volume 4, Number 13, pp. 1305-1314 © Inter-national Research Publications House http://www. irphouse.com

[6] M. Tariq Banday (2011). Easing PAIN with Digital Signatures" International Journal of Computer Applications (0975 – 8887) Volume 29– No.2

[7] Vagner Schoaba, Felipe Eduardo Gomes Sikansi, LuizCastelo Branco (2011). Digital Signature for Mobile Devices: A New Implementation and Eval-uation" International Journal of Future Generation Communication and Networking Vol. 4, No. 2

[8] Stallings W., "Cryptography and Network Security 4th Ed," Prentice Hall, PP. 58-309, 2005.

[9] Arpan K Kar Cryptography in the Banking Industry .https://www.researchgate.net/publication/26940 5090, © Business Fron-tiers Vol. 1, No. 1.

[10] D. Mahto and D. K. Yadav (2015). Enhancing security of one- time password \using elliptic curve cryptography with biometrics for e-commerce applications," in Computer, Communication, Control and Information Tech-nology (C3IT).Third International Conference on. IEEE, pp. 1–6.

[11] D. Mahto and D. Yadav (2015). Enhancing security of one-time password us-ing elliptic curve cryptography with finger- print biometric," in Compu-ting for Sustainable Global Development (INDIACom), 2nd Inter-national Conference on, March 2015, pp. 1737–1742.

[12] V. S. Miller. Use of elliptic curves in cryptography," in Advances in Cryptology CRYPTO 85 Proc., ser. Lecture Notes in Computer Science,

[13] H. Williams, Ed. Springer Berlin Heidelberg (1986) vol. 218, pp. 417–426.