www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 11 Issue 08August 2022, Page No.25553-25563
ISSN: 2319-7242 DOI: 10.18535/ijecs/v11i08.4671

A Finger Vein Pattern Based Key Generation Exchange And Security Framework For Iot Using Id Based Cryptography, Ecdh And Aes

Dnyaneshwari P.Wagh [1]
[1] Ph.D Student, Srtmu,Nanded, Maharashtra, India
Dnyaneshwari.Wagh15@Gmail.Com

Fadewar H.S [2]
Assistant Professor, School Of Computational Sciences, Srtmu,Nanded, Maharashtra, India
Fadewar_Hsf@Yahoo.Com

Shinde G. N [3]
Principal (Professor Grade), Yeshwant Mahavidyalaya, Nanded
Shindegn@Yahoo.Co.In

Santosh P. Shrikhande[4]
Assistant Professor, School Of Technology,Swami Ramanand Teerth Marathwada University, Nandedsub-Centre, Latur
Santoshshrikhande@Gmail.Com

Abstract:-
Every person has a unique finger vein pattern existing within each finger. Unlike facial features or fingerprints, finger vein authentication systems aren’t vulnerable to forgery. Finger vein authentication systems are more secure and reliable, and less expensive, than biometric security systems using fingerprint. This paper presents a novel security framework based on finger vein pattern. Finger vein pattern in used in id based cryptography to generate the keys for data encryption. These keys are combined with generator of elliptic curve cryptography (ecc) to exchange the keys using diffie hellman key exchange algorithm. Once the keys are exchanged, the data is encrypted using advance encryption standard (aes). This framework is tested in internet of things (iot) environment for enhancing the security. The iot based security systems implemented in the banks and other organizations can be enhanced considerably using the proposed security model.

Keywords: Finger Vein, Id Based Cryptography, Elliptic Curve Cryptography (Ecc), Diffie Hellman Key Exchange, Advance Encryption Standard (Aes), Iot.

Introduction:-

In Recent Years, Digital Businesses That Utilize Data Obtained From Various Devices Are Expanding To Meet The Rapidly Changing Markets And Customer Demands. On The Other Hand, Due To Insufficient Security Of Devices Connected To The Network, The Risk Of Damage From Cyber-Attacks Such As Unauthorized

Access, Eavesdropping / Falsification Of Communication Data, And Denial Of Service Is Increasing.In Order To Utilize Iot Systems Safely, It Is Necessary To Take Security Measures That Take Into Consideration The Characteristics Of Iot Systems, In Addition To The Conventional Security Measures For Information Communication And Technology (Ict) Systems. In Addition, Since Security Measures In Current Iot Systems Are Centered on The Cloud Layer, Security Measures For The Edge Layer And Device Layer Are Also Required. Concepts, Policies, And Concrete Methods Required For Security Measures In Cyber-Physical Systems (Systems That Can Affect Both Cyberspace And Physical Space (Real World)). An International Standard For Industrial Automation And Control Equipment And Development Processes That Companies That Manufacture And Operate Control Systems Should Address Regarding Security. Based On This Situation, Nec Has Set The Security Measures Required For The Edge Layer And Device Layer As "(1) Remote Management And Automation Of Device Security Settings", "(2) Access Control Corresponding To Various Device Connection Methods", And "(3) Abnormalities".

This Edge Device Records And Manages Manufacturing History (Parts, Inspection Information, Etc.) And Distribution History As A Trail On The Blockchain, Ensuring Its Own Authenticity. As A Result, For Example, Cameras And Gates Used For Entering And Exiting Face Recognition In Offices, Building Equipment Management Such As Air Conditioning And Elevators, And Devices That Are Attracting Attention In The " Guidelines For Cyber Physical Security Measures In Building Systems" Issued By The Ministry Of Economy, Trade And Industry. - Contributes To The Management Of Iot Devices Such As Industrial Controls That Require Security Considerations At The Component Level.

● **Iot Device Security Manager**: Permit List Type Access Control / Anomaly Detection Software That Protects Customer Systems From Various Threats That Occur On The Edge Of Iot And Devices. In Addition To Being Able To Automatically Create Access Control Settings For Each Device Distributed In Large Numbers In The Field, Which Is Difficult To Do Manually, In Addition To Being Able To Remotely Visualize The Connection And Communication Status Of Iot Devices In The Field, Iot Systems You Can Reduce Security Risks.

● **Lightweight Program Tampering Detection**
Software That Enables Tampering Detection Of Programs Running On Devices With Limited Hardware Resources Such As Sensor Devices And Devices Equipped With (Embedded) Linux.

● **Lightweight Encryption Development Kit**
Software That Enables High-Speed Encryption And Tampering Detection Even For Devices With Limited Hardware Resources Such As Sensor Devices.

● **Secureware / Credential Lifecycle Manager**
Device Id, Encryption Key (Public Key / Common Key), And Electronic Certification Required For Mutual Authentication And Encryption To Prevent Unauthorized Connections In Iot Systems Where Edges And Devices Are Distributed. Software That Enables The Creation And Management Of Books.

● **Privileged Id Management Solution For**
Iot Systems This Is A Solution That Extends The Integrated Id Management Software Product "Webcam Secure master / Enterprise Identity Manager Privileged Id Management Option" To The Edge And Devices Of Iot Systems. It Is Possible To Remotely Change The Default Administrator Id / Password Of The Edge Or Device To An Id / Password With High Security Strength And Manage The Granting Of The Usage Authority.

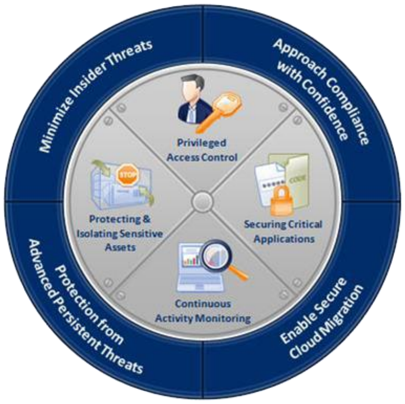

Minimize Insider Threats
Approach Compliance with Confidence
Privileged Access Control
Protecting & Isolating Sensitive Assets
Securing Critical Applications
Continuous Activity Monitoring
Protection from Advanced Persistent Threats
Enable Secure Cloud Migration

Figure 1: Iot Security Model

Given The Current Situation, The Potential Risk Of Cyber-Attack Cases Is Likely To Increase.Under The Leadership Of The Management, Each Financial Institution Should Deepen Its Awareness Of The Threat Of Cyber-Attacks And Take The Following Measures To Strengthen The Measures. In Addition, Overseas Bases May Also Serve As A Foothold For Cyber-Attacks On Important Domestic Systems, So Please Implement Security Measures With Specific Support And Instructions In The Same Way As Domestic Systems.

If Find Any Suspicious Movements, Please Report Them To The Department In Charge Of The Financial Services Agency / Finance (Branch) Bureau Immediately.

1. Measures To Reduce Risk:

- Strengthen Personal Authentication By Confirming Whether The Password Is Not Simple, Confirming Access Authority, Using Multi-Factor Authentication, Deleting Unnecessary Accounts, Etc.
- Understand The Holding Status Of Information Assets Including Iot Devices. In Particular, Vulnerabilities In Devices That Control The Connection To The Internet, Such As Vpn Devices And Gateways, Are Often Exploited In Attacks, So Security Patches (Latest Firmware, Updates, Etc.) Should Be Applied Promptly.
- Inform The Organization About Not Opening Email Attachments Carelessly, Not Clicking Urls Carelessly, And Promptly Contacting And Consulting.

2. Early Detection Of Incidents

- Check Various Logs On The Server, Etc.
- Re-Check Communication Monitoring / Analysis And Access Control.

3. Appropriate Response And Recovery In The Event Of An Incident:-

- Confirm The Data Backup And Recovery Procedure In Case Of Data Loss.
- In Preparation For An Incident, Confirm The Coping Procedure When The Incident Is Recognized, And Prepare An External Response And Internal Communication System.

II. Literature:-

Novak Et Al., (2018) [1] The Author Presents The Smart Mobile Devices Iot Application. The Security Of Mobile Devices Such As Smartphones That Work With Iot Is Now A Particular Point. While Downloadable Applications Such As Mobile Devices Are Easy To Use, They Are Less Secure Than Embedded Software, And The Challenge Is How To Protect Certificates And Rights Keys.In Particular, The Threat Has Increased Recently As Features Such As Network Connectivity, Application Additions, And Dynamic Application Updates Have Been Enhanced. In Order To Respond To This Threat, It Is Important To Take Security Measures For The Application Itself.

Banik, Et Al., (2017) [2], The Author Presents The "Analysis Of Software Countermeasures For Whitebox Encryption. Effective Technologies As Security Measures Are "Obfuscation" And "Confidential Encryption Key". By Utilizing The Software Protection "Code Protection" And "Whitebox" Of Verimatrix Co., Ltd., It Is Possible To Realize Tampering Check, Strong Obfuscation And Confidentiality Of Encryption Key. This Can Enhance The Security Of Various Applications That Handle Personal Information, Such As Financial Transactions And Id Management.

Kim Et Al., (2018) [3] The Author Introduce, Anti-Reversible Dynamic Tamper Detection Scheme Using Distributed Image Steganography For Iot Applications An Attacker Who Aims To "Tamper With" Software Could Use The Obtained Mobile Application To Perform Dynamic Analysis On The Emulator To Try To Understand The Detailed Behavior Of The Application. This Is Because If The Detailed Operation Can Be Clarified, The Application Can Be Tampered With Pinpoint. Attackers Can Also Hack And Confuse Many Users. These Security Threats Require "Tamper Detection" And "Obfuscation" Techniques.

Zeng Et Al., (2019) [4] The Author Presents The Code Protection Protects Application By Checking For Tampering At Runtime And Obfuscating Code. Code Protection Allows To Place Check Routines Within Application That Check For Tampering At Runtime. The Tool Can Also Automatically Determine That The Check Routine Should Be Placed In The Most Secure Location Without Impacting Performance And Can Be Embedded In The Application. In Addition, A High Degree Of Obfuscation Is Achieved By Combining Various Obfuscation Methods Such As Complicated Conditional Expressions, Changes In Control Structures Such As Loop, And Insertion Of Junk Code.

Shi, Et Al., (2021) [5] The Author Presents The Secure And Efficient White-Box Encryption Scheme For Data Protection Against Shared Cache Attacks In Cloud Computing. The Software Is Analyzed Dynamically, It Is Difficult To Protect The "Key" Used Inside The Software With Normal "Obfuscation". Depending On The Iot Device, It Is Possible To Protect Such A "Key" By Using Hardware. However, In Devices That Do Not Have Such Hardware, It Is Necessary To Keep The "Key" Used In The Software Safe. One Of The Solutions Is "Whitebox". Whitebox Technology Provides Strong Protection By Encrypting Sensitive Information Such As Encryption Keys Embedded In Software. Because The Software Is Translated At The Source Code Level, Even If An Attacker Dynamically Analyzes The Software And Looks At Its Contents, It Cannot See Sensitive Information.Whitebox Technology Will Slow Down A Bit, But It Will Definitely Protect Sensitive Information. If It Can't Protect Your Keys With Hardware, Whitebox Technology Is Considered The Best Solution For Security.

Saba Rehman Et Al. [6] Proposed A Secure Scheme For Sharing Data While Maintaining Data Security And Integrityover The Cloud. The System Mainly Functions By Combining The Ecc And The Advancedencryption Standard (Aes) Method To Ensure Authentication And Data Integrity.

Yasin Et Al [7] Stated That Hundreds Of Sensors Are Present In The Applications That Are Usedwhich Share Our Private Data With Other Objects Without The User’s Knowledge. Encryption Systems Can Be Used To Prevent This Emerging Security Problem. However, It Is Difficult To Determine The Appropriate Encryption System Due To Limited Power Resources And Computational Capabilities. In Their Study, An Identity-Based Encryption System Has Been Proposed For Secure Communication Between Objects Included In The Internet Of Things.

Jayawardana Et Al [8] Proposed A Hybrid Encryption Protocol Performs Both Asymmetric And Symmetric Ciphers. Advanced Encryption Standard (Aes) Is Used For Symmetric Cipher As It Is Proved To Be Highly Secured, Fast, And Well-Standardized, And Well Supported. They Joined Elliptic Curve Cryptography (Ecc) As Asymmetric Cipher Because It Is The Latest And Best Cipher Algorithm That Uses Smaller Keys And Signatures.

Zhiyong Luo Et Al. [9] Proposed A Technique To Improve The Efficiency Of Identification Analysis Under The Premise Of Ensuring Information Security, A Safe And Efficient Analytical Encryption Method For Industrial Internet Identification Based On Secure Hash Algorithm 256 (Sha-256), And Rivest-Shamir-Adleman (Rsa) Is Presented. Firstly, By Replacing The Secret Key In The Identification Encoding Encryption With The Sha-256 Function, The Number Of Secret Keys Is Reduced, Which Is Beneficial To Improve The Efficiency Of Identification Analysis. Secondly, By Replacing The Large Prime Number Of The Rsa Encryption Algorithm With Multiple Small Prime Numbers, The Generation Speed Of Rsa.

T. Sujithra Et Al. [10] Proposed A Method To Improve The Security On The Cloud.The Combined Approach Tdes Based Rsa Is Used To Prevent The Data From Theunauthorized Access. From The Experimental Results It Has Been Identified That Theproposed Method Provides Much More Security From The Traditional Methods.

Zia Bashir [11] Has Proposed The Scheme Of Asymmetric Key With The Use Of Elliptic Curve

Cryptosystem (Ecc). By Using The Method Of Dhk Sharing, The Sender And Receiver Will Be Agreed On The Elliptic Curve, But The Generator G Is Considered As Secrete And Its Hash Value As The Shared Parameter Publicly. Based On The Hash Value, The G Value Can Be Recovered By The Authorized Members. The Key Protocol Has Become Robust Than The Existing Method As The G Is Kept As Private.

Balasubramanian Prabhu Kavin [12] Has Proposed The Security Algorithm, I.E. The Elliptic Curve And Diffie-Hellman Based On The Mechanism Of Data Storage Or Ec(Dh)2 For The Cloud. Like Dh2, The Diffie-Hellman Is Used Twice And Is Combined With The Elliptic Curve Cryptography Standard Algorithm For Secured Storage In The Cloud Based Iot Environment.

III. Proposed Method:-

The Proposed Method Is Designed To Create Encryption Keys Form Users Finger Vein Patterns. This Iot Based Security Framework Enhances The Security Of The User. The Process Begins With The Concept Of Id Based Encryption Where The Conventionally The User's Mail Id Or Phone Number Is Used In The Process Of Key Generation. In The Proposed Method The User's Finger Vein Is Used To Generate The Key As Described In Algorithm I. This Key Is Treated As Private Key And The Public Key Is Generated Using The Concepts Of Elliptic Curve Cryptography. The Public Keys Are Exchanged Using Efficient Diffie Hellman Key Exchange Procedure. The Keys Are Used To Encrypt The Data Using Aes. Thus, The Proposed Algorithm Is Categorized As Hybrid Encryption Scheme. Figure 2 Shows The Architecture Pf The Proposed Model.

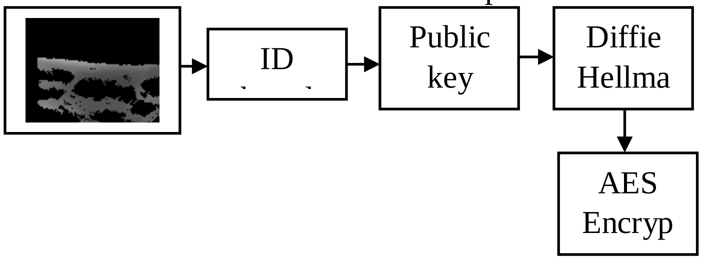


Figure 2: Proposed Model

3.1 Data Set:

Wildcat 640 From Xenics Wildcat 640 Is A Small, High Performance Ingaas Camera With Low Noise And High Dynamic Range. The Wildcat 640 Series Is Based On An In-House Developed, Temperature Stabilized Ingaas Detector With A 320x240 Pixel Resolution. The Camera Is Available With A Usb3 Vision Or A Cameralink Interface.

3.2 Id Based Encryption:-

Id-Based Cryptography Is A Model In Which Electronic Information Record Information Can Be Shared Between Organizations In The Region Based On An Id Like Mail Id, Serial Number Or Phone Number. Compared To The Existing Key Management Method, The Model Using Id-Based Encryption Has Many Major Advantages. Id-Based Cryptography Uses An Arbitrary Id That Each Individual Has Which Can Then Be Used To Generate A Public Key. This Is A Solution To The Problems Of Operation And Management After The Introduction Of A New One, And The Problem Of Cost At Each Information Institution Where The Introduction Of An Electronic Information Record System. In Other Words, Creating A System To Which Id-Based Cryptography Is Applied Will Lead To Cost Reduction And Solve The Cost Problem.

Algorithm 1: Key Generation Using Id Based Cryptography

```
Step 1: Read The Input Finger Vein Image
Step 2: Convert The Image Into A Column Vector
Step 3: Convert The Data Into A String.
Step 4: Remove The Spaces In The Strings If They Exist
Step 5: Create A Hash Object And Use Sha256 On The Input String.
Step 6: Convert The Output To Hexadecimal Notation
Step 7: Use The Data To Construct The Private Key
```

A Regional Information Record Management Server Will Be Established For Each Region As A Server That Manages All Information Record Information In That Region. There, The Index Information Of Information Records In The Area (When The Information Records Of Users Were Created And Saved) Is Centrally Managed. The Index Information Is Assumed To Be Based On The User Id (Finger Vein Pattern).Each Organization Sends Encrypted Information To The Regional Information Record Management Server On A Regular Basis. At This Time, The Organization Encrypts The Private Information With Its Own Organization Public Key And Sends It To The Regional Chart Management Server, And The Regional Chart Management Server Decrypts It Using The Organizationpublic Keyand Stores The Private Information.

The Flow When Anorganization Wants To Refer To The Information Records Of Other Organizations Of Users Is Described Below.

Step1: The Organization Accesses The Regional Information Record Management Server And Enters The User's Information Search The Records.

Step 2: The Requested Organization Encrypts The User's Information By The User's Public Key And Sends It To The Regional Chart Management Server

Step 3: Regional Chart,The Management Server Decrypts The Sent Data With The Public Key Shared Using Diffie Hellman Key Exchange And Shows The Encrypted Information Record To The Requesting Organization.

In Step 2 And 3**,** The Organization Can Only View The User's Chart On The Regional Chart Management Server Where The User's Private Key Can Be Obtained By Encrypting It With The User's Public Key When Extracting It From The Server.

3.3 Elliptic Curve Diffie-Hellman:

Elliptic Curve-Based Diffie-Hellman (Ecdh) Key Exchange Has Become The Recommended Method For Asymmetric Encryption In Recent Years, Notably In “Suite B” Released By The Nsa In 2010, Which Completely Excludes Protocols Based On Rsa Or Discrete Logarithm (Dsa).The Nsa Recommends The Use Of Ecdh With 256-Bit Or 384-Bit Keys Depending On The Level Of Confidentiality Of The Information. A Key Size Of At Least 256 Bits For Ecdh. Given Its Operation, The Ecdh Protocol Requires Keys Of Much Smaller Size Than Its Predecessors While Ensuring The Same Level Of Security. It Is Advisable To Use 256-Bit Keys For Ecdh When Paired With 128-Bit Aes, While Rsa Requires A 3072-Bit Key To Provide Equivalent Security.

Key Exchange Protocol

The Key Exchange Takes Place As Follows:

- Agreement Between A And B On The Parameters Of The Curve And A Common Point P (Generator) Chosen At Random On This Curve.
- Id Based Signature Is Used To Generate The Keys And These Correspond To Their Private Key (Pra Is The Private Key Of A, Prb Is The Private Key Of B).
- Public Keys Are Generated Using The Concept Of Ecc. (Pua = P * Pra, Pub = P * Prb)
- A Sends Pua To B. B Also Sends Its Public Key Pub Generated From Its Private Key Prb.
- A And B Can Now Calculate The Shared Secret (Pua*Pub)*P.
- The Key Used For The Actual Encryption Of The Communication (With Aes) Is Generated From A Hash Of The Shared Secret.

Security:

It Is Commonly Accepted That The Security Of This Exchange Relies On The Fact That It Is Easy To Calculate Pua And Pub From P, Pra And Prb, But That It Is Impossible To Find The Private Keys K From The Public Elements P, Pua And Pub.

Indeed, No Method Making It Possible To Solve The Discrete Logarithm On The Elliptic Curve (Therefore Finding Pra From Pua And P) Is Known Publicly To Date.At First Glance, It Seems Simple To Find “By Hand” Since The Scalar Multiplication Is Carried Out Very Quickly By The

Two Protagonists. However, The Calculation Of The Point Q (P * Pra) Is Based On Optimizations Which Make It Possible To Greatly Reduce The Number Of Intermediate Points To Be Calculated (A Bit Like Fast Exponentiation For Key Exchanges Based On The Discrete Logarithm). An Exhaustive Search For K From Q And P Implies A Calculation Of Each Possible Point Q And Therefore A Calculation Time Putting This Solution Out Of Reach.

3.4 Aes :

Aes Is 128-Bit Text Data Of Indefinite Length In Order From The Beginning. It Is Common To Each Block By Dividing It Into Blocks Of The Length Of A Common Key Block Cipher That Encrypts And Decrypts With A Key. To. In The Encryption Process, The Same Encryption Process As Des Repeat The Reason Many Times. The Number Of Repetitions, The Unit Is Expressed In Columns.

The Following Three Are The Main Features. Also, These Properties Other Than These Characteristics Are Shown In The Following Sections Common Key Block Cipher 128bit Block Length Can Be Used. Key Length Can Be Selected From 128bit, 192bit, 256bit

Block Length, Key Length, Number Of Rounds:

Des And Aes Block Length, Key Length, And Number Of Rounds. As Shown In Table 4, The Number Of Rounds Of Aes Depends On The Key Length. It Exists. Aes Makes Block Length And Key Length Longer Than Des By Doing So, Brute Force Attack, Ciphertext Match Attack, Dictionary Consideration Is Given To Ensure Sufficient Security Against Attacks.

Aes Is A Symmetric Block Cipher. It’s Plaintext Block And Ciphertext Block Are 128 Bits (16 Bytes), And The Key Length Is Usually 128 Bits (Or 192 Bits, 256 Bits, Etc.), And N Is Performed According To The Key Length. Round Operation, Usually When The Key Is 16 Bytes, N=10, 24 Bytes, N=12, 32 Bytes, N=14, The Following Is The General Encryption Process Of Aes:

Among Them, The 128-Bit Plaintext Is Represented By A Fourth-Order Matrix, And It Is Encrypted Into A 128-Bit Ciphertext After N Rounds Of Operations. In The N Rounds Of Operations, Each Round Undergoes 4 Transformations (The Last Round Is 3 Transformations): Byte Substitution, Row Shift Bit, Column Confusion And Round Key Addition. During The Encryption Process, The M-Bit Key Will Also Be Expressed In Matrix Form And Expanded Into The Key To Each Round (The Key Of Each Round Is Different, And It Is Transformed From The Previous Key), The Following Is M=128, N=10 As An Example To Introduce Aes Is The Specific Encryption And Decryption Process. There Are Two Important Parts In The Encryption And Decryption Process:

- **Plain Text Transformation**: The Specific Transformation Process Of Byte Substitution, Row Shift, Column Confusion And Round Key Addition
- **Key Expansion**: The Expansion Operation Of The Key And The Formation Of A Subkey

The Following Will Introduce The Specific Structure And Transformation Function Of Aes Using A 16-Byte Key And 10 Rounds Of Transformation. At First Glance, Aes Has Many Transformations, And The Key Expansion Process Is Very Complicated.

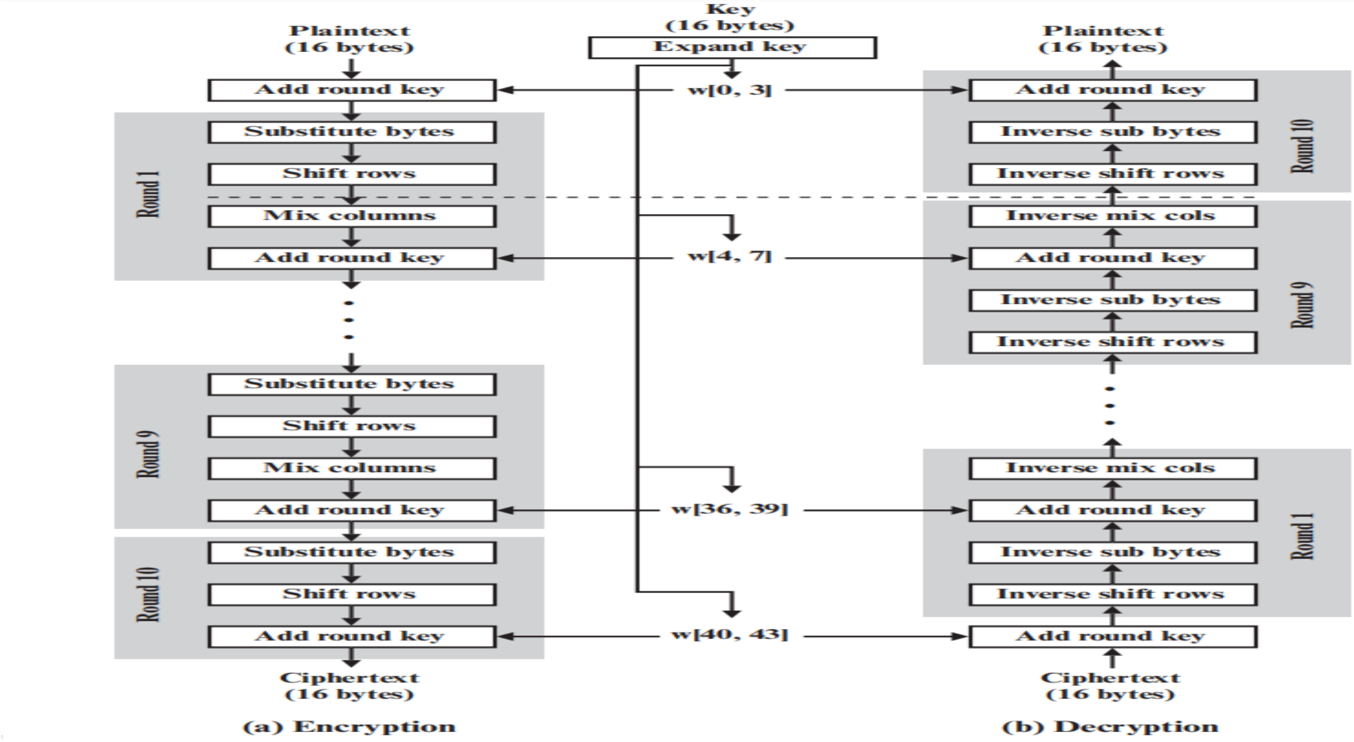
The Encryption Process And Decryption Process Of Aes Using A 16-Byte Key Are Shown In Figure 4.9. It Can Be Seen That Although Aes Uses A Large Number Of Substitution And Permutation Operations Like Des, It Does Not Use Feistel Structure Like Des, Because Aes Is Plaintext It Is Not Divided Into Left And Right Parts But Expressed In Matrix Form.

For The Transformation Of Plaintext And Ciphertext In The Encryption And Decryption Process, The Plaintext Is First Subjected To Round Key Addition Operations, And Then Undergoes 10 Rounds Of Substitution And Permutation Transformations:

- **Substitute Bytes**: Use An S Box To Complete The Byte-To-Byte **Substitution Of The** Packet
- **Shift Rows**: A Simple **Replacement**

- **Column Confusion (Mix Columns)**: The Use Of Finite Fields Gf(28)An **Alternative** To The Above Arithmetic Features (The Last Round, That Is, The 10th Round Is Not Confused)
- **Add Round Key**: Perform Bitwise Xor Operation On Part Of The Current Grouping And Expansion Keys

The Above Four Stages Are All Reversible, And Because Of This, There Is No Obfuscation Calculation In The Last Round (The 10th Round).Also Worth Noting Is The Generation Of Round Keys. Initially, The 16-Byte Key Was Expanded To Generate A 176-Byte Key And Divided Into 11 Groups W [0,3], W [4,7],..., W [40,43]. These Keys Are Also Used For The Round Key Addition In Encryption And Decryption Operations. In The Following Example, You Can Find That The Round Keys For Each Round Are Different.



(a) Encryption

(b) Decryption

Figure 3: Encryption And Decryption Process Of Aes With 16-Byte Key

IV. Experimental Results

The Experimental Results Show The Performance Analysis Of The Proposed System. The Proposed System Is Fast And Secure And Can Be Integrated Into Iot Systems For Enhanced Security. The Analysis Is Performed In Terms Of: Key Generation Time, Total Key Length, Encryption Time, Throughput And Avalanche Effect.

Key Generation Time – Key Generation Time Is The Time, Which Means Time Taken By The Method To Generate The Key.

Total Key Length – The Generated Key Is Represented In Bytes.

Encryption Time – Time Taken By The Process To Encrypt Input Data To Encrypt The Data.

Decryption Time – Time Taken By The Process To Decrypt Encrypted Data Back To Input The Data.

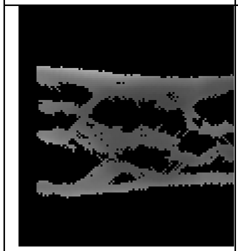
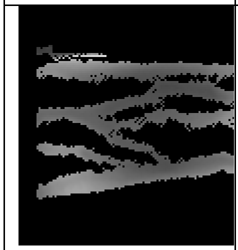
Throughput – The Ratio Of The Total Encrypted Plaintext In Bytes And Encryption Time.

Avalanche Effect – The Cipher-Text Is Significantly Changed Due To The Slight Change In Either The Plain-Text Or The Key. It Is Called As Avalanche Effect.

Table 1 Shows The Encryption Results Obtained From Persons 1 And 2. Two Persons Finger Vein

Image Patterns Are Loaded As Inputs (A), (B). The Images Are Used To Generate The Private Keys Shown In Column 2. In Column 3, The Final Encryption Keys Given To Aes Are Shown.

Table 1: Encryption Results

Image	**Private Key**	**Reduced Final Encryption Key**
 (a) Input Finger Vein Image Of Person 1	18c705fb1a7dd0956 E24d989f08629e310bb 204157b34d62e641c1 F926b1f0e8	107daa57105ac400000000
 (b) Input Finger Vein Image Of Person 2	E490afe9ce7e42f 3a30059dc8468f 0b37e2786d36e20a82 B8a97d737887c1fe4	107daa57105ac400000000

The Table 2 Shows The Performance Evaluation For The Proposed Method. The Table Includes Key Generation Time, Total Key Length, Encryption Time, Decryption Time Throughput And Avalanche Effect.

Table 2: Performance Evaluation For The Proposed Method

Parameters	
Key Generation Time(Sec)	0.176780
Total Keys Length(Bytes)	24
Encryption Time (Sec)	0.035700
Decryption Time(Msec)	0.029524
Throughput(Bytes/Sec)	672.26
Avalanche Effect(%)	50

When Compared To Existing Methods, The Key Generation Time Is Less In The Proposed Method. The Total Key Length Is Reduced By The Proposed Key Length Reduction Procedure. The Reduction In The Key Length Has Reduced The Encryption Time And Decryption, Encryption Memory Usage And Decryption Memory Usage. The Throughput Has Increased Because Of The Reduction In Encryption Time.

Conclusion

A Unique Security Framework Based On Finger Vein Pattern Is Presented In This Paper. In Id-Based Cryptography, The Finger Vein Pattern Is Utilised To Produce Keys For Data Encryption. These Keys Are Used In Conjunction With An Ecc Generator To Exchange Keys Using The Diffie Hellman Key Exchange Algorithm. The Data Is Encrypted Using Advance Encryption Standard When The Keys Are Exchanged (Aes). This Framework Is Being Used To Improve Security In The Internet Of Thigs (Iot). The Key Generation Time Is 0.176780 Seconds While The Total Keys Length24 Bytes. The Encryption Time 0.035700 Seconds And The Decryption Time Is 0.029524seconds. Throughput Is 672.26bytes/Sec And The Avalanche Effect Is 50%.

Reference:-

1. Novak, Ed, Zhuofan Tang, And Qun Li. "Ultrasound Proximity Networking On Smart Mobile Devices For Iot Applications." *Ieee Internet Of Things Journal* 6, No. 1 (2018): 399-409.
2. Banik, Subhadeep, Andrey Bogdanov, Takanoriisobe, And Martin Bjerregaard Jepsen. "Analysis Of Software Countermeasures For Whitebox Encryption." *Cryptology Eprint Archive* (2017).
3. Kim, Sung Ryoung, Jeongnyeo Kim, Sung Tae Kim, Sunwoo Shin, And Jeong Hyun Yi. "Anti-Reversible Dynamic Tamper Detection Scheme Using Distributed Image Steganography For Iot

Applications." *The Journal Of Supercomputing* 74, No. 9 (2018): 4261-4280.

4. Zeng, Qiang, Lannan Luo, Zhiyun Qian, Xiaojiang Du, Zhoujun Li, Chin-Tser Huang, And Csilla Farkas. "Resilient User-Side Android Application Repackaging And Tampering Detection Using Cryptographically Obfuscated Logic Bombs." *Ieee Transactions On Dependable And Secure Computing* 18, No. 6 (2019): 2582-2600.
5. Shi, Yang, Mianhong Li, Wujing Wei, Yangyang Liu, And Xiapu Luo. "Secure And Efficient White-Box Encryption Scheme For Data Protection Against Shared Cache Attacks In Cloud Computing." In *2021 Ieee 32nd International Symposium On Software Reliability Engineering (Issre)*, Pp. 446-456. Ieee, 2021.
6. Rehman, Saba, Nida Talat Bajwa, Munam Ali Shah, Ahmad O. Aseeri, And Adeel Anjum. "Hybrid Aes-Ecc Model For The Security Of Data Over Cloud Storage." *Electronics* 10, No. 21 (2021): 2673.
7. Genç, Yasin, And Erkan Afacan. "Identity-Based Encryption In The Internet Of Things." In 2021 29th Signal Processing And Communications Applications Conference (Siu), Pp. 1-4. Ieee, 2021.
8. Jayawardana, H. P. T. M., And R. L. Dangalla. "Hybrid Encryption Protocol For Rfid Data Security." In *2020 International Conference On Decision Aid Sciences And Application (Dasa)*, Pp. 1209-1212. Ieee, 2020.
9. Luo, Zhiyong, And Bo Wang. "A Secure And Efficient Analytical Encryption Method For Industrial Internet Identification Based On Sha-256 And Rsa." In 2022 Ieee 6th Information Technology And Mechatronics Engineering Conference (Itoec), Vol. 6, Pp. 1874-1878. Ieee, 2022.
10. Sujithra, T., M. Sumathi, And M. Ramakrishnan. "Id Based Adaptive-Key Encryption Using Tdes And Rsa For Data Security In Cloud Environment."
11. Bashir, Zia, M. G. Malik, Muhammad Hussain, And Nadeem Iqbal. "Multiple Rgb Images Encryption Algorithm Based On Elliptic Curve, Improved Diffie Hellman Protocol." Multimedia Tools And Applications 81, No. 3 (2022): 3867-3897.
12. Kavin, Balasubramanian Prabhu, And Sannasi Ganapathy. "Ec (Dh) 2: An Effective Secured Data Storage Mechanism For Cloud Based Iot Applications Using Elliptic Curve And Diffie-Hellman." International Journal Of Internet Technology And Secured Transactions 10, No. 5 (2020): 601-617.
13. C. Liu, S. Ruan, Y. Lai And C. Yao, "Finger-Vein As A Biometric-Based Authentication," In Ieee Consumer Electronics Magazine, Vol. 8, No. 6, Pp. 29-34, 1 Nov. 2019, Doi: 10.1109/Mce.2019.2941343.
14. Jianfeng Zhang, Zhiying Lu, And Min Li. "Active Contour-Based Method For Finger-Vein Image Segmentation." *Ieee Transactions On Instrumentation And Measurement* 69, No. 11 (2020): 8656-8665.
15. Zenin J.Vásqucz-Villar, Juan J. Choquehuanca-Zevallos, Jimmy Ludeña-Choez, And Efraínmayhua-López. "Finger Vein Segmentation From Infrared Images Using Spectral Clustering: An Approach For User Indentification." In *2020 Ieee 10th International Conference On System Engineering And Technology (Icset)*, Pp. 245-249. Ieee, 2020.
16. Simonkirchgasser, Christof Kauba, Yen-Lung Lai, Jinzhe, And Andreas Uhl. "Finger Vein Template Protection Based On Alignment-Robust Feature Description And Index-Of-

Maximum Hashing." *Ieee Transactions On Biometrics, Behavior, And Identity Science* 2, No. 4 (2020): 337-349.

17. Babakmaser, And Andreas Uhl. "Identifying The Origin Of Finger Vein Samples Using Texture Descriptors." *Arxiv Preprint Arxiv:2102.03992* (2021).
18. Minalmadankar, S. D. Sawarkar, And D. J. Pete. "Biometric Privacy Using Various Cryptographic Scheme." In *2018 Ieee Global Conference On Wireless Computing And Networking (Gcwcn)*, Pp. 159-162. Ieee, 2018.
19. Rudreshdwivedi, Somnathdey, Mukulanand Sharma, And Apurvgoel. "A Fingerprint Based Crypto-Biometric System For Secure Communication." *Journal Of Ambient Intelligence And Humanized Computing* 11, No. 4 (2020): 1495-1509.
20. Sanjay Shekhawat, Heinz Hofbauer, Bernhard Prommegger, And Andreas Uhl. "Efficient Fingervein Sample Image Encryption." In *2020 8th International Workshop On Biometrics And Forensics (Iwbf)*, Pp. 1-6. Ieee, 2020.
21. L. Nishaevangelin, And A. Lenin Fred. "Securing Recognized Multimodal Biometric Images Using Cryptographic Model." *Multimedia Tools And Applications* 80, No. 12 (2021): 18735-18752.
22. Sanaibjaoun, Anasabou El Kalam, Vincent Poirriez, And Abdellah Ait Ouahman. "Biometric Template Privacy Using Visual Cryptography." In *International Conference On Innovations In Bio-Inspired Computing And Applications*, Pp. 309-317. Springer, Cham, 2017.