International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 4 Ver. V|| April 2018 || PP 51-54

Design of Three Tier Architecture for Near Field Communication

Nisha.G.S. Mrs.Geetha.M.R.
Pg Student, Communication And Networking,Ponjesly College Of Engineering,
Ponjesly College Of Engineering.
Assistant Professor,Department of ECE,Ponjesly college of Engineering.
Corresponding Auther: Nisha.G.S.

Abstract-*Near Field Communication (Nfc) Has Been Used For Short Range Communications In A Number Of Applications For Consumer Electronics Devices. Specifically, Nfc Has Been Used In Electronic Payment Systems. In This The Trusted Service Manager Will Provide The Tag To Users And They Will Exchange It. The Tag Is Created From User A's Information, User B's Information, Trusted Service Manager's Information.* This *Paper Describes A Digital Image Watermarking Scheme Using Discrete Wavelet Transform. In This Scheme, Digital Image Watermarking Algorithm Is Based On The Dwt Coefficients. It Combines The Information Of Low Frequency Dwt Coefficients And The Watermark Image. This Combination Is Used As Input For Extraction Of The Watermark. Watermark Extraction Can Be Simply Done Because The Proposed Algorithm Does Not Change Any Information Of The Original Image. Quality Of The Original Image Remains Unaffected.*

Index Terms *- Near Field Communication; Trusted Service Manager; Digital Image Watermarking; Verification Tag.*

Date of Submission: 10-04-2018 Date of acceptance: 26-04-2018

I. Introduction

With The Advancements In Short-Range Wireless Communication Technology, The Near Field Communication (Nfc) Technology Is Being Used At Large Scale Both From Academia And Industry. The Communication Distance Of The Nfc Technology Works Nearly Up To 4 Inches. Its Operating Frequency Is 13.56 Mhz With The Transmission Speed Range From 106 Kbps To 424 Kbps. Various Smart Devices Have Been Widely Used And Are Also Expected To Be Continuously Used In The Internet Of Things (Iot) Environment. The Combination Of The

Smart Devices And Nfc Technology Expands The Use Of The Smart Devices In A Number Of Applications, Such As Service Discovery, E-Payment, Ticketing, And So On. Especially, According To Research Reports, The Market Size Of Nfc-Based Payment Services Would Be Increased To $3.572 And $180 Billion In 2015 And 2017 Separately.

Objects Of Nfc Could Be Divided Into Initiator And Target Objects. An Initiator Object Generates A Radio Frequency Field And Starts The Nfc Interface. After Receiving Communication Signals, A Target Object Sends A Response Message To The Initiator Object Through The Radio Frequency Field. However, Due To The Shared Nature Of Wireless Communication Media, The Nfc Technology Is Vulnerable To Many Kinds Of Attacks. Security Is Thus One Of The Most Important Issues For The Nfc Technology.

II. Existing System

After Receiving The User *A*'s Request For Pseudonyms, The Trusted Service Manager (Tsm) Generates *N* Pseudonyms And Sends Them To *A* Through A Secure Channel. The Tsm Also Stores The User *A*'s Identity And Pseudonyms Into Its Database.

When The Initiator User *A* And The Target User *B* Want To Communicate And Generate A Session Key, The Following Steps Will Be Executed As Shown In Fig(1).

1) First Step Is To Select The Appropriate User.
2) Nfc User Interface Has Opened For The Selected User.
3) User A Has Been Selected And User A Going To Load The1d Data, Using Load Data Menu Of The

Graphical User Interface. Similar To The User, A User B Load The 1d Data On The Other End.
4) 1d Data Has Been Successfully Loaded By Both Of The Users. Acknowledgement Has Been Opened In The Nfc Gui.

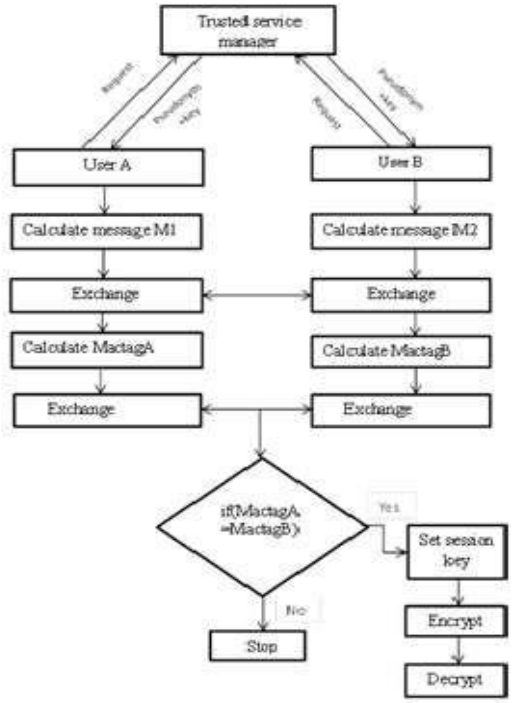

Figure.1.Three Tier Architecture For 1d Data

5) Pseudonym Has Been Created By The Trust Manager And Back To The Users.
6) After Pseudonym Has Been Created By Trust Manager The Message Has Been Created For The Respective Users.
7) After The Message Has Been Created By Both Users The Messages Has Been Exchanged Between The Users.
8) After The Message Has Been Exchanged By Both Users The Tags Has Been Created And Exchanged Between The Users.
9) After The Tags Of Both Users Are Matched The Session Key Has Been Created And Data Is Ready For Encryption.
10) Encryption Of Data File That Has Been Loaded Initially By The Users.
11) The Session Key Has Been Created And Data Is Ready For Decryption.
12) Decryption Of Data File Has Been Done And The
Nfc Is Successfully.

III. Security Analysis

Security Analysis Results That Security Are Provided In Terms Of Mutual Authentication, User Anonymity, Session Key Security And Perfect Forward Security. In Addition, The Protocol Could Withstand Impersonation Attack, Replay Attack, Man- In The-Middle Attack And Modification Attack When Compare To The Previous Protocols.

IV. Proposed System

As Per Three Tier Architecture The Data Transfer From One User To Another User With The Knowledge Of Trusted Third Party.
1) First Step Is To Upload The Host Image On The Initiator Object.
2) In The Initiator Object, Uploading The Secret Image Which Is Going To Transmitted To The Target Object.
3) Secret Image Is Transformed Into Wavelet Domain Using Discrete Wavelet Transform. Dwt Decomposes The Image Into The Sub-Bands Such As Ll, Hh, Lh And Hl.Dwt Coefficients Are Obtained From Sub-Bands We Get The Decomposed Image.

4) Digital Watermarking Algorithm Based On Dwt Is Used. This Algorithm Combines The Mutual Information Of Decomposed Image And The Host Image From That We Get The Water Marked Image.
5) While Embedding The Mutual Information Tag Is Generated From The Tsm.
6) Entering The Generated Tag Value, Confusion And Diffusion Parameters We Get The Lsb Watermarked Image
7) Based On The Tag Value, Confusion And Diffusion Parameters We Can Encrypt The Watermarked Image As A Result We Get The Encrypted Image.
8) On The Target Object, Encrypted Image Generated On The Initiator Object Is Used As The Input.
9) Entering The Tag Value Which Is Already Generated On The Initiator Object And Also Entering The Same Confusion And Diffusion Parameter Value After That We Get The Decrypted Image (I.E.) Water Marked Image.

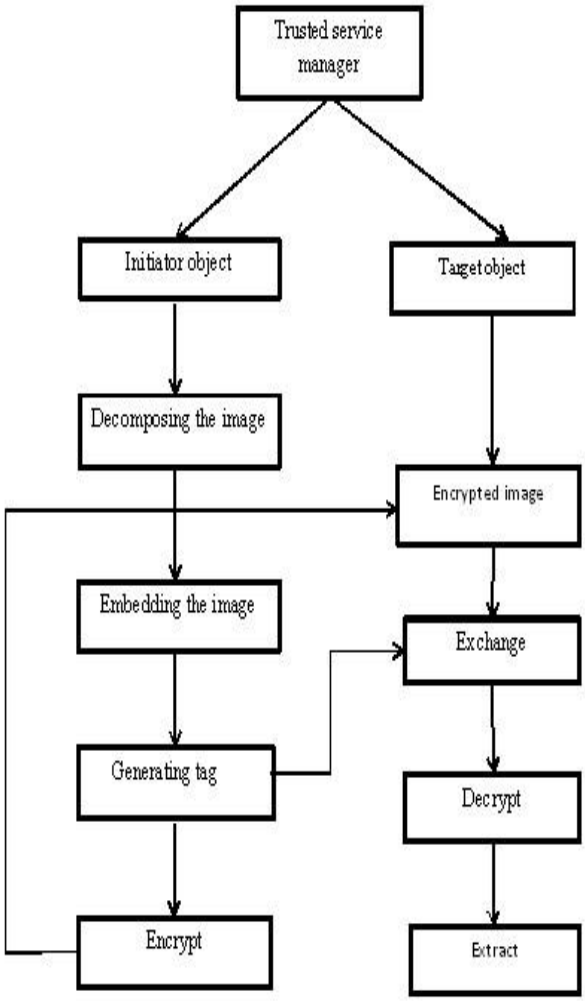

Figure.2.Three Tier Architecture For 2d Data

10) After Getting The Decrypted Image, By Applying Inverse Discrete Wavelet Transform To The Decrypted Image We Can Extract The Secret Image From It.

V. Conclusion

This Paper Provides The Novel Approaches For Implementing Digital Image Steganography, That Is To Conceal Secret Information Inside An Image So That It Invisible To The Eyes. This Paper Provides Efficient Steganography Methods, So That The Person Can Find The Variety Of Choosing The Method To Protect The Information. In Image Domain, We Discussed The Most Powerful Technique Called Lsb To Hide Information Particularly Inside A Bmp File

Format Whereas In Transform Domain Powerful Dct (Discrete Cosine Transform) Was Discussed. Wavelet Based Digital Image Watermarking Scheme By Embedding Watermark With Low Frequency Area Of Wavelet Domain Has Been Proposed. A Digital Image Watermarking Scheme Using Discrete Wavelet

Transform Is Implemented. Watermark Image Is Simply Extracted Because The Proposed Algorithm Does Not Change Any Information Of The Original Image. Quality Of The Original Image Remains Unaffected. Proposed Digital Image Watermarking Scheme Has Been Implemented Using Matlab Software.

References

[1] Altaaf O. Mulani, Priyanka R. Kulkarni," Robust Invisible Digital Image Watermarking Using Discrete Wavelet Transform"2015, International Journal Of Engineering Research & Technology,Issn: 2278-0181,Vol. 4 Issue 01,January-2015.

[2] Ajay Jadhav, Shashikala Channalli," Steganography-An Art Of Hiding Data"Shashikala Channalli Et Al /International Journal On Computer Science And Engineering Vol.1(3), 2009, 137-141.

[3] Calandriello.G, Papadimitratos.P, Hubaux.J.P, And Lioy.A ," Efficient And Robust Pseudonymous Authentication In Vanet," Proceedings Of The Fourth Acm International Workshop On Vehicular Ad Hoc Networks, 2007 Pp. 19-28.

[4] Chatterjee.S ,Das.A.K And Sing.J.K, "An Enhanced Access Control Scheme In Wireless Sensor Networks," Ad Hoc & Sensor Wireless Networks, (2014)Vol. 21, No. 1-2, Pp. 121-149.

[5] Debiao He, Jong-Hyouk Lee,Neeraj Kumar," Secure Pseudonym-Based Near Field Communication Protocol For The Consumer Internet Of Things"Ieee Transactions On Consumer Electronics, 2015vol. 61, No. 1, February 2015.

[6] Dipalee Gupta, Siddhartha Choubey,"Discrete Wavelet Transform For Image Processing" International Journal Of Emerging Technology And Advanced Engineering,Issn 2250- 2459, Iso 9001:2008 Certified Journal, (2015) Volume 4, Issue 3, March 2015.

[7] Eckhoff.D, Sommer.C, Gansen.T, German.R, And Dressler.F, "Strong And Affordable Location Privacy In Vanets: Identity Diffusion Using Time-Slots And Swapping," Proceedings Of The 2010 Ieee Vehicular Networking Conference, (2010) Pp. 174-181.

[8] Eun.H, Lee.H,Oh.H, Conditional Privacy Preserving Security Protocol For Nfc Applications, Ieee Trans. Consumer. Electronics, (2013) Vol. 59, No. 1, Pp.153-160.
Gartner, "Market Insight: The Outlook On Mobile Payment," (2010) Market Analysis And Statistics.

[9] Guo.H,.Teo.J.C.M.Ngoh.L.M, "An Anonymous Dos- Resistant Password-Based Authentication, Key Exchange And Pseudonym Delivery Protocol For Vehicular Networks, Proceedings Of The 2009 International Conference On Advanced Information Networking And Applications, (2009)Pp. 675-682.

[10] [10] He.D,Kumar.Mandlee.J.H,"Anonymous Two-Factor Authentication For Consumer Roaming Service In Global Mobility Networks," Ieee Trans. Consumer. Electronics, (2013)Vol. 59, No. 4, Pp. 811- 817.

[11] He.D,Zhang.Y,Chen.J,"Cryptanalysis And Improvement Of An Anonymous Authentication Protocol For Wireless Access Networks," Wireless Personal Communications, (2014)Vol. 74, No. 2, Pp. 229-243.

[12] He.D And Wang.D,"Robust Biometrics-Based Authentication Scheme For Multi-Server Environment, (2014)"Ieeesystemsjournal,Doi: 0.1109/Jsyst.2014.23015.

[13] He.D,Wu.S, "Security Flaws In A Smart Card Based Authentication Scheme For Multi-Server Environment," Wireless Personal Communications, (2013)Vol. 70, No. 1, Pp. 323-329.

[14] Ho.P.H Lin.X ,Lu.R, Shen.S.H,Zhu.H, "Ecpp: Efficient Conditional Privacy Preservation Protocol For Secure Vehicular Communications," Proceedings Of The27th Conference On Computer Communications (Infocom 2008), ,(2008) Pp. 1229-1237.

[15] Huang.D,Misra.S,Verma.M,Xue.G, "Pacp: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol For Vanets," Ieee Transactions On Intelligent Transportation Systems, (2011) Vol. 12, No. 3, Pp. 736-746.

[16] Iso/Iec 15946-1, "Information Technology – Security Methods–Cryptographic Methods Based On Elliptic Curves – Part 1: (2008) General, Iso/Iec".

[17] Iso/Iec 13157-1, "Information Technology Telecommunications And Information Exchange Between Systems – Nfc Security – Part 1: Nfc-Sec Nfcip-1 Security Service And Protocol," (2010) Iso/Iec.

[18] Iso/Iec 13157-2, "Information Technology Telecommunications And Information Exchange Between Systems – Nfc Security – Part 2: Nfc-Sec Cryptography Standard Using Ecdh And Aes," (2010) Iso/Iec.

[19] Iswaryar.J,Poornima.R,"An Overview Of Digital Image Steganography"International Journal Of Computer Science & Engineering Survey (Ijcses) (2013) Vol.4, No.1,February 2013.

[20] Lin Li, Zhu Yuefeng," Digital Image Watermarking Algorithms Based On Dual Transform Domain And Self-Recovery" International Journal On Smart Sensing And Intelligent Systems, (2015) Vol. 8, No. 1, March 2015.

Nisha.G.S."Design Of Three Tier Architecture For Near Field Communication " International Journal of Engineering Science Invention (IJESI), vol. 07, no. 04, 2018, pp 51-54