Data Mining Techniques For Security Maintenance Using Multi Level Dependency

Sri. E. Ramesh[1], Dr. A. Sri Nagesh[2]

[1]Assistant Professor, Department of CSE, RVR & JC College of Engineering, Guntur, Andhra Pradesh

[2]Associate Professor, Department of CSE, RVR & JC College of Engineering, Guntur, Andhra Pradesh

Abstract— Presently, Smart phones are generally utilized as a part of everyday life. Individuals utilize them to store exceedingly imperative information including email, secret key, money related records points of interest like charge card number, ledger number and therapeutic records and so forth. With the ascent in advanced mobile phones and their inherent sensors and also web applications, an expanding measure of private information is by and large quietly got to. Android framework gives office to store android application information and other data on google cloud and synchronize this information with our application while utilizing application. Yet, this transmission in broad daylight correspondence framework isn't secure a result of block attempt and uncalled for control. These makes android framework as an essential stage for security protecting application. Along these lines, elective answer for this issue is to served multilayer security to information. In this paper, we give multilevel security to our information to influence framework more to secure. One of the primary targets of these framework is to pre vent from decent variety assault and other non-straight assaults. To give multilevel security we join cryptography and steganography approach. The advantage of these plan is that steganography can work on encoded content and subsequently it offers a twofold layer information assurance and power for secure information transmission over an open channel.

Keywords- **security preserving; Multilevel dependancy; synchronization; Data mining;**

I. INTRODUCTION

Protection is a noteworthy issue when information contains some delicate information. On the off chance that we apply nonlinear crash assault on existing framework, it is conceivable to recreate unique information. The proposed work is focus on multilevel trust. Presently a-days the vast majority of people groups utilizes android cell phones and individuals utilize them to store their imperative information like charge card number, ledger number, email locations and passwords or some business related information and so on. As android mobiles give office to store their information on google cloud on the web. Under this administration, pernicious information excavator may approach that information while information transmission occurred. Various suspicious assaults like assorted variety and nonlinear assault may focused on this information. As the this information transmission isn't secure android is an essential stage for protection safeguarding. The answer for this existing approach are restricted in their unsaid presumption of single-level trust on information excavators. The answer for these issue is to served multilevel security while exchanging information.

In proposed framework, we are going to served to multilevel security to information. To guarantee multilevel security we consolidate cryptography and steganography approach. At the point when information is exchanged fro m sender to beneficiary, In first level, cryptography is utilized. Subsequent to applying cryptography the emit information can be changed over in encoded arrange, that is indiscernible to outsider. Concealed message is scrambled utilizing symmetric key algorithm that is Blowfish algorithm. In second level, picture steganography is utilized. This enables the clients to safely conveying the information. The main undertaking of the Steganography is to nourish client adaptability of passing the data, executing the encryption measures according to the determination and calculations proposed and store the data which is in imperceptible shape. Picture steganography is method of concealing presence of discharge information by keeping it into another medium, for example, picture. Utilizing steganography the encrusted information is taken cover behind a picture. The key based recovery office is use to recover the shrouded information at recipient side. In proposed framework, multilayer security is given to information and along these lines, nobody separated from sender and expected collector recognize the existence of message. The advantage of these approach is that steganography can connected on encoded writings and subsequently it bolsters a double layer information insurance. This framework upgrades security of client's touchy data or information or some vital documents by joined science of steganography and cryptography to fulfill necessity of security and power for secure information transmission over a station

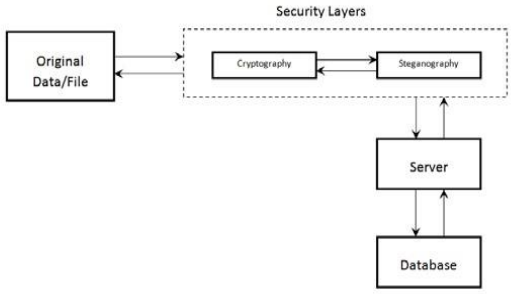


Figure 1

The framework covers a various put stock in levels for information to give security. Right off the bat, the first information is send from sender side to planned client. Utilizing Cryptography this information gets changed over into encoded information. On this encoded information picture steganography is connected. Utilizing this the information is covered up by picture and send to server. This framework has an inversion procedure, which is utilized to deembed the information from picture document and then unscramble the information to its unique arrangement as indicated by the demand by the client. To retrive the concealed subtle elements of information the key based recovery strategy is utilized. While performing Encryption and Decryption, the application ought to fulfill the norms of approval and verification of the client.

II. RELATED WORK

Privacy preserving is a major issue in recent years. There are number of existing system for security of private data. Previously there are so many approaches are defined for privacy preservation of data. As per the research done by Seema Kedar and few others, they have designed concept of existing privacy preservation of data mining techniques & how to achive their effeiceincy [1]. This survey on PPDM can be helpful for finding the limitations of existing data mining approaches. It ensures efficient privacy preservation of data.

The restriction of available sytem is distinct level confidence on information miners. At next level, Perturbing the data values for preservation of customer privacy is used [2]. The study of perturbation based Privacy Preservation of Data Mining technique introduces new method which is random perturbation that is number of changes made in the original data.

III. CRYPTOGRAPHY

Cryptography is the craft of utilizing arithmetic to encode and unscramble information. It changes over a content into incoherent organization. Cryptography permits to store emit information of client or exchange it to approved individual in encoded arrange that can be confused by anybody aside from the approved beneficiary. It is an antiquated craft of composing the emit code. The way toward attempting to break any figure instant message to get the first message itself is known as cryptanalysis. While cryptography is the craft of securing information, cryptanalysis is the art of investigating and breaking secure correspondence. Established cryptanalysis includes an intriguing mix of logical thinking, utilization of numerical instruments, design discovering, persistence, assurance, and luckiness.

IV. STEGANOGRAPHY

Steganography is an approach of concealing the way that correspondence is going on. It can be achive by hidding unique data behind some other data. Steganography is study of concealing the data by installing the message in another record. It might be picture, sound, video document and so forth. Steganography push to conceal the Perturbation based protection conservation approach bothers the right information with some another sort of known irregular clamor and exchange the boisterous information to the information excavator. The field of irritation based protection safeguarding is explained to multilevel security utilizing a multilevel trust situation by where the annoyed duplicates of same information is accessible at different trust levels [5]. Here, Additive bother approach is utilized where irregular commotion is added to real information with subjective appropriation.

In the examination by Vaishali Borade, R.N.Phursule, they had examined on the off chance that we apply nonlinear plot assault on MLT-PPDM approach, it is conceivable to remake unique data.[6] When same nonlinear agreement assault is connected on proposed framework it can't reproduce unique duplicate information implies it safeguard the protection. In that work, they may apply nonlinear methods to determine unique information and recoup more data. Under the multilevel trust situation, at more elevated amounts information mineworkers can get to less bothered duplicates. In any case, these less annoyed duplicates are not open by information excavators at bring down confide in levels. At various put stock in levels, information diggers may interest to share the bothered duplicates among themselves. Thus, it is traditional that information diggers approach more than one irritated duplicate. In this, security is saved if covering commotion straight change calculation which produces clamor into unique information. What's more, when same nonlinear assault is connected then unique information can't be reproduce.

Security protecting intended to anticipate data exposure and guarantee legitimate access to the information. In this manner, protection safeguarding is distinctive fro m existing information security, get to control and encryption innovation which tries to forestall data divulgence against illegitimate means.The significance of Personal information covering up has been brought up in different applications. One of the prevalent methodologies for data stowing away is steganography. This approach utilized by R. Valarmathi and G. M. Kadhar Nawaz builds framework security by utilizing steganography with encryption along with key management.[4] Here One more approach of giving multilayer security to client's close to home information presented by mrs. Rabbit Ram Sah and Gunasekaran. In burrow ital security the undeniable advantage of steganography over encoded information is that, this messages don't draw in consideration of information mineworkers to themselves, to couriers or to recipient.[3].

V. METHODOLOGY

A. SYSTEM ARCHITECTURE

The above figure outline the segments of framework.

- User Login: Here, client right off the bat logon to the framework.
- User database: It contains client's close to home information or some other data.

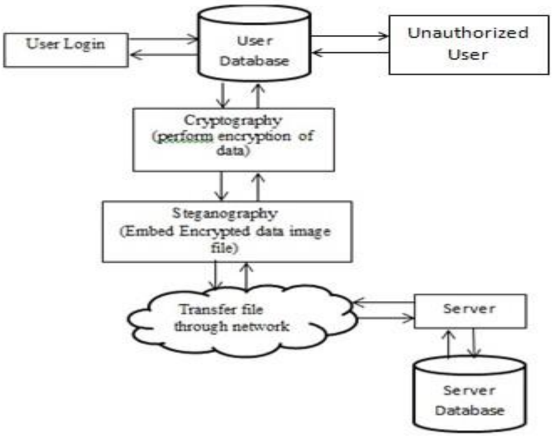

User Login
User Database
Unauthorized User
Cryptography (perform encryption of data)
Steganography (Embed Encrypted data image file)
Transfer file through network
Server
Server Database

Figure 2: System architecture

- Cryptography: It is use to secret unique message from client to indistinguishable frame that is encoded design.
- Steganography: Here, the utilization of steganography is to insert a message which is in scrambled configuration into picture document to conceal the first information. Also, this resultant picture document is exchange to server.
- Server database: It stores all the client related information.
- Unauthorized client: He is malevolent client or information digger who tries to get to client's close to home data or different points of interest.

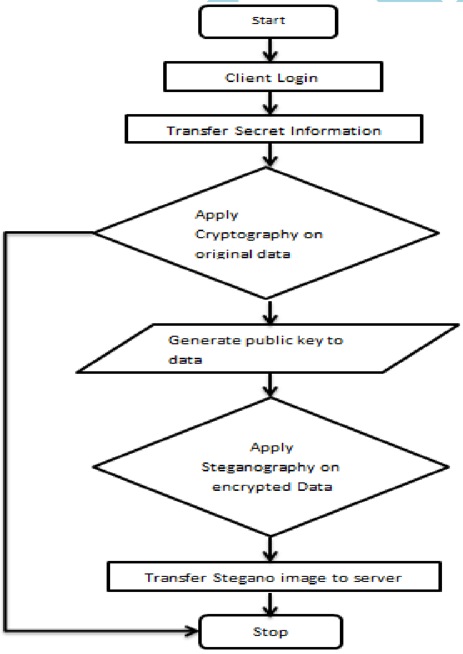
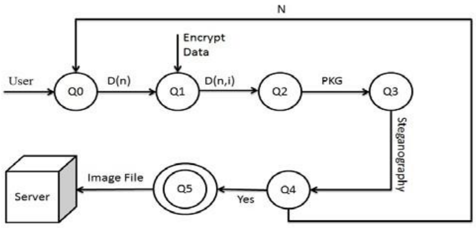

Start
Client Login
Transfer Secret Information
Apply Cryptography on original data
Generate public key to data
Apply Steganography on encrypted Data
Transfer Stegano image to server
Stop

Figure 3:System Workflow

B. SYSTEM W ORKFLOW

The above framework work process delineates the framework usefulness that can be taken out in stream. Right off the bat, client logins to the framework. He played out his work. At the point when client needs to exchange a few information or some emit data to another client. That time this data may hacked by malevolent information excavators. As a result of these, on this emit data cryptography is connected first. which can exchange this discharge message into encoded organize. After that on this encoded information steganography is connected. Utilizing this system the encoded message is installed in some another picture record. As a result of which client can't foresee the presence of discharge data. What's more, this data is send to the foreordained beneficiary.

C. MATHEMATICAL MODEL



So the above machine can be additionally expounded as: Let,

S= {Q0,Q1,Q2,Q3,Q4,Q5} Q0= {D(n)}

Q1 = {D(n,i)} Q2 = {PKG} Q3 = {SG}

Q4 = {successful hiding} Q5 = {Si}

Where 'S' is the principle set of states through which the framework

will go through it's life-cycle and the information will go through the regarded states.

Where,

Q0 = Data Set [D(n)]

Where 'Q0' is where the fundamental informational index is put away on which the handling required to be done to give the protection on the information on different levels as per necessities.

Where,

Q1 =Encrypted Data Set [D(ni)]

Where 'Q1' is where unique information which is to be send is changed over into encoded arrange.

Where, Q2 = Applying open key age on encoded information [PKG]

Where 'Q2' is where people in general key age strategy is required to additionally encode the multi-level security.

Where,

Q3 = steganography[SG]

Where 'Q3' is where the steganography is utilized over an encoded information. What's more, this encoded information is hidded behind picture

Where,

Q4 = fruitful Hidding.

Where 'Q4' is where it checks whether both Steganography and cryptography is sucessfully connected to actuall information or not..

Where,

Q5 = Stegano_Image[Si]

Where 'Q5' is where stegano picture is send as a picture document to the server.

So by the shortenings above, we can get

Stegano_image=Stegano_image{encrypt}

So the previously mentioned calculation can be utilized on the total informational index to give the multi-level protection on the client's Confidential informational collection.

VI. PROCEDURE

A. Procedure for installing emit information inside picture.

- Input: Secrete_data.
- Output: Stegano_Image.

Stage 1 : Choose the Text record containing the mystery message.

Stage 2 : Encrypt the content record substance utilizing Blowfish Algorithm.

Stage 3 : Select the Image petition for installing the mystery message.

Stage 4 : Embed the encoded emit information behind a picture. Stage 5 : Send the picture document to the beneficiary.

B. Procedure for retrieving emit information from picture.

- Input: Stegano_Image, Secrete_ Key.
- Output: Secrete_data.

Stage 1 : Choose the Embedded Image petition for e xtracting the mystery message.

Stage 2 : Extract the mystery information from Image record.

Stage 3 : If mystery message exhibit in Image document at that point show the message to the end client after extract ing message. Else show that no concealed information is available.

Stage 4 : Decrypt the mystery information utilizing Blowfish Algorithm.

Stage 5 : Display the discharge information to the end client.

VII. CONCLUSION

Information Security is a critical issue now-a-days. The current advances for Privacy safeguarding of information are great upto some e xtend. Be that as it may, to keep from decent variety assault and other nonlinear assaults and furthermore for greater upgrade, we proposed the above framework that has been configuration to give a multilevel security to client's emit information while exchanging. The cryptography and steganography are utilized for multilevel security. The reason for this plan is that the steganography can connected on encoded information, as a result of this the framework offers double layer information assurance. The consolidated approach of both these procedures give vigorous and secure information transmission.

REFERENCES

[1] Seema Kedar, Sneha Dhawale, Wankhade Va ibhav, Pavan Kadam, Siddharth Wani, Pavan Ingale, “Privacy Preserving of Data Min ing “International Journal of Advanced Research in Computer and Communication Engineering Vo l. 2, Issue 4, April 2013.

[2] Yaping Li, Minghua Chen, Qiwei Li, And Wei Zhang, “Enabling Multilevel Trust In Privacy Preserving of Data Mining”, IEEE Transactions On Knowledge And Data Engineering, September, 2012.

[3] Hare Ram Sah And G. Gunasekaran, “ Privacy Preserving Collaborative Data Mining Using Steganography And Encryption “, Journal Of Theoretical And Applied Information Technology, 31st October 2014.

[4] R.Vala rmathi ,M.Phil, G.M.Kadhar Nawa z, “Information Hiding Using Audio Steganography with Encrypted Data”, International Journal of Advanced in Computer and Communication Engineering Vo l. 3, Issue 1, January 2014.

[5] Kamaleswari S, Balachander T, “Handling Non-Linear Attacks in Mult ileve l Trust Privacy Preserving in Data Mining”, Kamaleswari S et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, 2014.

[6] Vaishali Bhorde, R.N.Phursule, “Imple mentation of Multi-Level Trust in Privacy Preservation in Data Mining against Non-Linear Attack “, International

Journal of Computer Applications (0975 – 8887) Volume 115 – No. 21, April 2015.

[7] TipawanSilwattananusarn and KulthidaTuamsuk, “Data Mining and Its Applications for Knowledge Management”, International Journal of Data Mining & Knowledge Management Process (IJDKP), Vo l.2, No.5, September 2012.

[8] Berson, A., Smith, S.J. &Thearling, K.,“ Building Data Mining Applications for CRM”, NewYork: McGraw-Hill, 1999.

[9] Lalitha P., Vidhushavarshini S., “Retrieving Information using Reversible Data Hiding”, International Journal of scientific research management, Vo l. 2, No. 5, pp. 802- 808, 2014.

[10] Puech, W., Erkin, Z., Barni, M., Rane, S.,Lagendijk, R.L., “ Emerging cryptographicchallenges in image and video processing”, Image Processing (ICIP), 19th IEEE International Conference, pp. 2629-2632, Sept. 2012.

[11] Lavrac, N., Bohanec, M., Pur, A., Cestnik, B., Debeljak, M. &Kobler, A., “Data mining and visualizat ion for decision support and modeling of public health-care resources”, Journal of Bio medical Informatics, 40, 438- 447, 2007.

[12] Rahman, N. & Harding, J.A., “Textual data mining industrial knowledge management and text classification: A business oriented approach”, Expert Systems with Applications, 39, 4729-4739, 2012.

[13] Abhishek Koluguri, Sheikh Gouse, P. Bhaskara Reddy, “Text Steganography Methods and its Tools”, International Journal of Advanced Scientific and Technical Research, Vo. 2, No. 4, pp. 888- 902, April 2014.

[14] Benny Pinkas, “Cryptographic techniques for privacy preserving in data mining”, SIGKDD Explorations, Vo l.4, Issue 2, pp. 12-19, 2002.

[15] AkanshaAgrawal, Virendra Singh, “Securing Video Data: A Critical Review”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 5, May 2014.

[16] Murat Kantarcioglu and Wei Jiang, “ Incentive Compatible Privacy-Preserving Data Analysis”, IEEE Transactions on Knowledge and Data Engineering, Vo l. 25, No. 6, June 2013.

[17] M. Kantarcioglu and O. Kardes, “Privacy Preservation of Data Mining in the Malicious Model”, International Journal of Information and Computer Security, Vo l. 2, pp. 353-375, Jan. 2009.

[18] L. Sweeney, “ K-anonymity: A Model for Protecting Privacy”, International Journal on Uncertainty, Fuzziness based Systems, pp. 557-570, 2002.

[19] SavitaLohiya, Lata Ragha, “Privacy Preserving in Data Mining Using Hybrid Approach”, Fourth International Conference on Computational Intelligence and Communication Networks, 2012.

[20] V. Vijayalakshmi, Mahalakshmi, Thamizharasan, “Data Encryption hiding technique in non-standard cover files”, International Journal of Advanced Research in Computer Science and Technology, Vol. 2, No. 1, March 2014.

[21] Jian Wang, Yong cheng Lou, Yen Zhao, Jiajin Le, “A Survey on Privacy Preserving Data Mining”, International Database Technology and Applications Workshop, pp.111-114, 2009.

[22] D. Agrawal and C.C. Aggarwal, On the Design and Quantificat ion of Privacy Pre-serving Data Mining Algorithms, Proc. 20th ACM SIGMOD-SIGA CT-SIGA RT Symp. Princip les of Database management Systems (PODS 01), pp. 247-255, May 2001.

[23] K. Chen & L. Liu, Privacy Preserving of Data Classification with Rotation Perturbation, Proc. IEEE Fifth Intl Conf. Data Mining, 2005.

[24] K. Liu, H. Kargupta & J. Ryan, “Random Projection-Based Multiplicative Data Perturbation for Privacy Preservation of Distributed Data Mining”, IEEE Trans. Knowledge and Data Eng,, Jan. 2006.

[25] Yehuda Lindell & Benny Pinkas, "Secure Multiparty Computation for Privacy-Preserving Data Mining," The Journal of Privacy and Condentiality, vol. 1, no. 1, pp. 59-98, 2009.