Prodrive- to share it with anybody else.

Business, Management

PRODRIVE- A PENDRIVE THAT PROVIDES DATA SECURITY AND PEN DRIVE TRACKING1A. Anandita Iyer, 2Preeti, 3B. Bharathi1, 2 Student, 3Professor1, 2, 3Department ofComputer Science & Engineering, SathyabamaInstitute of Science and Technology,,,

in ABSTRACTThe easiest way to store data and to achieveportability of data, pen drive is widely used. Different forms of data can bestored in the pen drive i. e., whether the data is in the form of document or inthe form of images anything can be stored.

The data stored in it can beconfidential and there may be chances that the owner of pen drive doesn't whatto share it with anybody else. Moreover pen drives are very small in size. Thereare chances that they are lost easily or can also be stolen easily.

We need tomake the data secure and provide some authentication in the pen drive so thateven when the pen drive is lost/stolen the access to pen drive is prohibited. The main focus of this project is to secure the data present in the pen drive. KEYWORDS Log Files, Encryption, RSA, AES, RF ID, GPS INTRODUCTION Data(audio, video, text, etc.) can be transferred to and from computer quickly withthe help of Pen drives. Data can easily be read and written by the user on thePen Drive by plugging it into the USB port on the computer. Due to the compactand portable nature of the pen drives they are widely used and they also don'trequire any external power supply.

Floppy disks and CD's are replaced by pendrives due to several benefits provided by the latter. Fast access and transferof data in addition with larger data storage is provided by pen drives. Storagecapacity of the Pen Drive can

vary from few megabytes to over 100 GB. Nowadayseven external hard drives are available in the market with huge storagecapacity, which like Pen Drive can be connected to a USB port on the computer. It is an external storage devicewhich can easily be lost. Sometimes the data stored in Pen drive isconfidential and important so if it is lost it can lead to severalconsequences. So our aim is to secure the data so even if somebody gets hold ofthe pen drive they are unable to misuse it. After securing the data it’snecessary to get our pen drive back.

To do so we need to track the location ofthe Pen drive. LITERATURESURVEY DATA SECURITYWhen comparedto fixed Winmax, mobile networks have high security architecture9, 12, becauseit is wireless and also very secured as it implements various protocols. Protocols like, Privacy and key management protocol version 2, X. 509certificate, Security Associations etc and also different encryption methods. Other ECC techniques with mobile networks can be also used so as to ensurestrong authentication. This along with RSA techniques ensure secureauthentication.

Uses RSA key encryptiontechnique. Splits the data into smaller encryption key. Hence encryption process is faster and easierto execute. Thereare two Cryptographic techniques mostly used, Secret-Key Cryptography andpublic key cryptography13, 5. Secret-Key Cryptography, also known as single-keyor private-key or symmetric key or one-key encryption technique. It uses one and same key for both encryption anddecryption side. If we use this technique, its cost is very less but has manydrawbacks like, shared secret key requirement, distribution of same key on bothsides, authentication and

non-repudiation. Inpublic-key cryptography which is also referred to as public key encryption, makes use of two different key on both encryption side and decryption side, i.

e. public key and private key respectively. Here, the public key is availableto all and is used in encrypting the messages. Whereas the private key is morelike a hidden key or a secret key, and is used to decrypt the message. RSAalgorithm uses multiple keys to perform encryption and decryption and hence ithelps in a very secure transmission of data and message. RSA algorithm works betterif the key value is large, because it will be difficult to find the factor ofn.

Asmentioned above, large key size helps better authentication. But it alsoconsumes space and wont be easy and user friendly. So to overcome this problema hybrid cryptographic technique 18, 15 has been prepared. It includes, RSA, DES and SHA1 algorithms. This is done majorly to enhance the encryption processand provide more security in key generation. This also helps in reducing keysize considerably and improving the key complexity.

This encryption techniqueis used in the JAVA environment. And the performance of hybrid encryption isassessed on the basis of encryption and decryption time and space complexity. Differentstudies has shown that AES algorithm6 works faster as compared to otherencrypting and decrypting algorithms. The encryption time of AES is very less compared to the encryption timetake by RSA. AES is more secured than RSA or DES or Tipple DES.

AES is morebetter, secure and faster algorithm to work with. Clouddata encryption techniques 2, 3 is based on file matching technique. It makesindexes of the stored file and supports a secure environment for user search. Further the file matching the keyword in the various searches and ranked basedon the relevant frequency and file length.

This also helps in solving theproblems of multi-keyword search on cloud data, and sets of different privacyrequirements. Among different multi-keyword semantics, by choosing theprinciple of coordinate matching to effectively represent similarity betweenquery keywords and outsourced documents, and using inner product similarity, the principle of similarity measurement. Studying some further enhancements ofthe ranked search mechanism, supports more search semantics, i. e., TF _ IDF, and dynamic data operations. Access control for the different users has beenachieved and the integrity check of data which is been outsourced to the cloudhas examined efficiently. It provides virtualized security to the data.

Itmajorly concentrates on data indexing and extracting. HARDWARE TRACKINGBarcodeScanning 8, 16, 17 helps in locating the pen drive. This can be implementedwith the help of a circuit which will be on the pen drive. The circuit isimplemented on Matlab Simulink as it gives an accurate result. And there is aGPS (in our phones) used with the barcode so that it becomes easy to track thepen drive. It is an added functionality that provides better result. Thecircuit attached to the pen drive contains a set of micro chip and microcontroller for data transmission and aseparate data logger to store pen drive information, i. e.

its longitudinallatitude information. Hence making itseasy to track the pen drive. The only drawback to the arrangement is that thepen drive should be properly charged. The circuit should have enough charge totransfer information to mobile gps

Fig 1. Block Diagram The figure1 is explained as; ATmega644: We use ATmega644to transfer data between hardware components present in the circuit.

Max2472: Weuse Max2472 to trace the location and to findout the latitude and longitude position of the device. Datalogger: Weuse Data logger for storing all the datathat is collected in the form of co-ordinates. The data will be sent to a datalogger and it will save that data. Rechargeableunit: To supply power to the circuit, we use a rechargeable unit. This rechargeable unit supplies the power to thecircuit. It will charge the USB device, when it will be connected to thesystem. RFID 1, 4, 14 can also be used for device tracking. It is a small chip whichsends the location of the device within a specified range.

The drawback with RFID is that, its perimeter range for device location is very small, i. e. 30-40meters. GPS vehicletracking System 7, 10, 11. This system makes use of the latitude and longitudeof the location of a vehicle which is to be tracked.

Google maps are beingused. The user makes the request for tracking the vehicle and the deviceresponds via SMS. The SMS contains of the latitude and longitude informationabout the vehicle and thus using it we can locate the vehicle on google maps. In addition to tracking, we can also perform

various functions remotely on thevehicle, like switching ON ignition system, switching it off too, locking thedoors of the vehicle and remotely unlocking the doors. Firstly, a signal issent by the user to the tracking system. As soon as the signal is received, thesystem tracks the vehicle and a SMS is sent to the user that contains the exactlocation. COMPARISON BETWEENVARIOUS ENCRYPTION ALGORITHMS Fewencryption algorithms are being compared on based of attributes like: key size, execution time, security level, block size etc.

Table 1: Encryption algorithm comparison Input Key Size Execution Time(ms) Security Level Block Size Asymmentric Cryptographic Algorithm 49 6. 456 Medium Level 64 Diffie-Hellman Key Exachage RSA ALGORITHM 36 3. 976 High Security 64 RSAAsymmetric Algorithm BLOW FISH 54 5. 998 High Security 128 SHA-224 DES ALGORITHM 123 6. 159 Medium Level 64 SHA-386 3DES ALGORITHM 256 0. 699 Very High Security 64 SHA-256 Proposed Method FEASIBILITY STUDY ECONOMICFEASIBILITYThe extra costapart from buying the pen drive is that of the GPS (micro GPS) which costsnearly about 600 rupees. Though it is more than the cost of pen drive but wecan compromise few bucks for it as it provides us the facility to locate ourlost pen drive.

If our pen drive is lost then definitely we will buy a new one. So despite of buying a new pen drive we can spend some money to buy a pen drivewith inbuilt GPS system. TECHNICALFEASIBILITYIn order toencrypt the data present in the pen drive we are going to use RSAencryption-decryption algorithm. It occupies space of nearly about 0. 5-0. 6 GBin the pen drive

which is approximately negligible. PRACTICALFEASIBILITYIn order to makethe pen drive to be used by everyone different security measures are provided.

If the pen driveis going to be used by corporate then in that case they can make use of the. EXE & LOG file security measure. But if pen drive is going to be used bysome common people like students etc.

then they can follow theusername-password security followed by encryption-decryption algorithm whichmakes the pen drive feasible. CONCLUSIONHence afterreferring various papers it can be concluded that, in the proposed project, thepen drive can be devised with a MINI GPSfor easy TRACKING of the pen drive. Andfor DATA SECURITY in pen drive, itcan be done in two ways: 1. Ifthe data is vulnerable and cannot be compromised at any cost, then . EXE FILE & LOG FILE approach isused. That is, the system will have the exe files installed, and the pen drivewill be having the IP address of the system saved in the log file. If the IPaddress is matched then only the system can access the data in the pen drive, or else a mail is sent to the owner and the drivers of the pen drive areblocked.

2. Ifthe USB is to be used among a group of people, then USERNAME-PASSWORD authentication will be provided. Then the datawill be encrypted and decryptedusing a KEY.

If the key is enteredwrong more than the specified number of times, then again information regardingunauthorized access is sent to the owner and the USB drivers are blocked. Accordingto the survey, it is found that the AESEncryption Technique is the most suitable technique to encrypt data.

REFERENCES 1. Ajinkya C Bapat, Sonali U Nimbhorkar ” RFID Based Object Tracking SystemUsing Collaborative Security Protocol” DOI 10. 4010/2016. 943 ISSN 2321 3361 ©2016 IJESC 2. AkshathaMS , Renita Tellis “ Cloud Data Encryption Using RSA, Enabling Multi-KeywordRanked Search and Achieving Privacy Requirements” International Journal ofAdvanced Research in Computer and Communication Engineering Vol. 5, Issue 5, May 2016 3.

Curtmola. R, Garay. J, Kamara. S, Ostrovsky. R.” SearchableSymmetric encryption: improved definition and efficientconstructions”.

In: proceedings of the 13th ACM conference on computer and communications security, pp. 79-88ACM(2006) 4. Darshankumar Dalwadi*, Insiya Guriwala, Shiwangi Chaudhary, Miloni Kapadia & Megha Savalia “ Implementation of Attendance System based onRFID and GSM with respect to Power Saving Concept” International Journalof Current Engineering and Technology E-ISSN 2277 – 4106, P-ISSN 2347 – 5161©2016 INPRESSCO®, All RightsReserved Available at http://inpressco.

com/category/ijcet 5. DhananjayPugila, Harsh Chitrala, Salpesh Lunawat, P. M. Durai Raj Vincent “ An efficeientencrpytion algorithm based on public keycryptography”, IJET , Vol 5 No 3 Jun-Jul 2013, pp. 3064-3067 6. Dr.

Prerna Mahajan & Abhishek Sachdeva, IITM, India, Global Journal of Computer Science andTechnology, Network, Web & Security, Volume 13 Issue 15 Version 1. 0 Year2013 7. Almomani, N. Alkhalil, E.

Ahmad and R. Jodeh, “ Ubiquitous GPS vehicle tracking andmanagement system,” in IEEE Jordan Conference on Applied ElectricalEngineering and Computing Technologies (AEECT), Amman , December 2011. 8. K. Lakshmi Sudha, Shirish Shinde, Titus Thomas “ Barcode based Student Attendance System” International Journal of ComputerApplications (0975 – 8887) Volume 119 – No.

2, June 2015 9. KR Chandrasekhara Pillai and M P Sebastian,” Elliptic Curve basedAuthenticatedSession KeyEstablishment Protocolfor High Security Applications in Constrained Network Environment”, International Journal ofNetwork Security & Its Applications (IJNSA), Vol. 2, No. 3, July 2010 10. M.

Parvez, K. Ahmed, Q. Mahfuz and M. Rahman, “ Atheoretical model of GSM network based vehicle tracking system,” inInternational Conference on Electrical and Computer Engineering (ICECE), Dhaka, 2010. 11. Mashood Mukhtar “ GPS based Advanced Vehicle Trackingand Vehicle Control System” International Journal of Intelligent Systems and Applications, 2015, 03, 1-12 Published Online February 2015 in MECS (http://www.

mecs-press. org/) DOI: 10. 5815/ijisa. 2015. 03.

01 12. Rajesh Yadav, S. Srinivasan, SunilGupta “ Security Analysis of RSA and ECC in Mobile Wimax” International conference on SignalProcessing, Communication, Power and Embedded System, 2016 13. Sarthak R Patel, Prof. Khushbu Shah, Gaurav R Patel “ Study on Improvements in RSAAlgorithm” Study on Improvements in RSA Algorithm|

ISSN: 2321-9939 14. Saravanan Sundaresan, Robin Doss" Secure Ownership Transfer in Multi-tag/Multi-owner Passive RFID Systems" Globecom 2013 – Symposium on Selected Areas in Communications 15.

Seyed Mohammad Seyedzadeh, SattarMirzakuchaki," A fast color image encryption algorithm based on coupled two-dimensional piecewisechaotic map", & 2011 Elsevier B. V. 16. Suhas Machhindra Gaikwad, Rahul Joshi, ShishirMachhindra Gaikwad " Find Out Pen DriveLocation with the Help of Mobile GPS" International Journal of Computer Applications (0975 – 8887) Volume 135– No. 2, February 2016 17.

Suhas Gaikwad: " CohortIntelligence and Genetic Algorithm along with AHP to recommend an Ice Cream toa Diabetic Patient". Lecture Notes In Computer Science, 12/2015: chapterCohort Intelligence and Genetic Algorithm along with AHP to recommend an IceCream to a Diabetic Patient: pages 1-9; SEMCCO 2015. 18. V. Kapoor Dept, Rahul Yadav " A Hybrid Cryptography Techniquefor Improving Network Security" International Journal of Computer Applications(0975 – 8887) Volume 141 – No. 11, May 2016