Securing Data inside Images in Rdbms for Protection against Cyber Attacks

A.V.A Swarna & Dr. K.Suresh Babu

[1]M.Tech Student, Department of CSE, School of Information Technology JNTUH, Village KPHB, Mandal Kukatpally, District RangaReddy, Telangana, India

[2]Senior Assistant Professor, Department of CSE, School of Information Technology JNTUH, Village KPHB, Mandal Kukatpally, District RangaReddy, Telangana, India

Abstract:

This project is largely written as an answer to the drawbacks of existing system. This project may be utilized in a true world application by any organization. Its can be used as a general secured application with few minor modifications. The aim of this project is to implement numerous advanced securing algorithms which are able to offer secure information storage to any or all varieties of knowledge the users and worker of BSNL contend with. The company is presently handling some encoding and cryptography algorithms. The matter is with knowledge that is susceptible to some terribly acquainted attacks like SQL injection attacks by that knowledge may be hacked. Therefore this project provides an answer for the issues caused by this type of attacks. By encrypting the info and by implementing steganographic strategies.

Introduction:

In today's world of rising technology, computers are enjoying an important role in each walk of life. The issues because of the normal system are overcome with the assistance of tasks being on-line. Securing of the information from varied attacks could be a massive concern currently. Aside from this, storage of the voluminous amounts of knowledge is tough. Moreover, the issues of consistency, reliableness, integrity conjointly exists. Since the storing of knowledge in databases there's perpetually likelihood that there's loss of knowledge, or manipulation of knowledge by unknown persons leading to less reliableness, durability. As these problems are of major concern, we've enforced some advanced security algorithms for storing of knowledge firmly were altogether the on top of factors ar achieved.

The main aim of this Project is to secure storage of information exploitation stereographic ways to store original data within pictures and resulting storage of those pictures in a very info. In this project we tend to use the smallest amount important bit (LSB) rule of stereography to cover information within the photographs so the trespasser if hacks the information base won't be ready to see the data gift. Here the info we tend to used is RDBMS. All the information is within the format of BLOB in MYSQL.

2. Steganography:

Steganography is that the follow of concealing messages or info inside different non-secret text or knowledge. It involves the activity of a secret message within AN innocent-looking package or instrumentation (often known as a carrier). as an example, a micro-dot hidden at a lower place a item, or a message written in milk on the rear of a letter, or directions tattooed beneath a personality's hair. Steganography is concerning exploitation steganographic techniques to cover text within PNG pictures. Steganography is typically confused with cryptography, since it is a closely connected plan. Cryptography scrambles a message; therefore associate uninvited reader is unable to know it. Steganography is concerning secrecy; therefore a possible hearer will not even apprehend there is a message to be scan. Stereography and cryptography will be combined to supply a hidden encrypted message – 2 levels of protection from prying eyes that is enforced victimization the Jasypt API (http://www.jasypt.org/). Another topic associated with Stereography is digital watermarking, that is used for tracing and distinctive digital media, like pictures, audio, and video. The cracking of Stereographic messages is named stegenalysis, and comes in 2 main forms. The simplest variety of cracking merely makes the hidden message unclear by modifying the carrier. This could typically be achieved by cropping or blurring the image, or saving it during a totally different file format. a far more durable task is that the extraction of the hidden message, which usually starts with the identification of tell- tale regularities or patterns within the carrier, or recognizing variations between the carrier and its original. Some basic steganalysis techniques victimization Image Java-based image process code square measure used.

1. Cyber Attacks

A cyber-attack is any style of offensive manoeuvre used by nation-states, people, groups, or organizations that targets laptop info systems, infrastructures, laptop networks, associated/or notebook computer devices by numerous means that of malicious acts typically originating from an anonymous supply that either steals, alters, or destroys a specific target by hacking into a inclined system.[1] These is tagged as either a cyber campaign, cyber warfare or cyber terrorism in numerous context. Cyber attacks will vary from putting in spyware on a computer to makes an attempt to destroy the infrastructure of entire nations. A Cyber Attack is associate attack initiated from a laptop against another laptop or an internet site, with a read to compromising the integrity, confidentiality or accessibility of target and therefore the info hold on in it. This text explains what square measure Cyber Attacks, its definition, sorts and talks regarding the way to stop them and therefore the course to require within the event of a cyber attack. Cyber Attacks, in a way, is generally thought of to be a region of Cyber Crime.

4. Existing System:

In the ancient system some basic encrypting and decipherment algorithms area unit used to secure knowledge in database management system. This existing system is prone various attacks. This is often as less secured and doesn't give reliable knowledge. The varied operations performed on these files like modifying and uploading of the records area unit terribly tedious. Thus, less sturdiness is achieved.

4.1 Disadvantage:

Security isn't provided and anyone will access, so any one can access it. The scope is proscribed to text files solely and large information like pictures fail to cover. SQL Injection attacks area unit less difficult so Image piracy cannot be avoided. Feasibility is reduced and less dependableness. Without any GUI and not user friendly. Only single system used, if the system crashes then the info is lost

5. Proposed System:

The projected system is developed supported stereographic methods, where the encrypted information is keep in a picture...it is keep in an exceedingly BLOB format in information. Thus reducing and protecting from cyber attacks. This starts by inquiring for user name and word that provides authentication. This technique provides high security wherever the unauthorized users cannot access the information. Later we've totally different choices for the worker like register for brand new user, uploading file, downloading file, storing some information.

5.1 Advantage:

Easy to use, effective and economical with accurate results, easy maintenance. fast access More practicableness and secure (Protection from SQL Injection Attacks) very troublesome for hacker to hack the information. Provides high consistency with reliability

6. Literature Survey:

6.1. C. Pu, "A world of opportunities: CPS IOT and beyond", *Proceedings of the 5th ACM international conference on Distributed event-based system*, pp. 229-230, 2011, July.

The sophistication and pervasiveness of cyber-attacks are constantly growing, driven partly by technological progress, profitable applications in organized crime and state-sponsored innovation. The modernization of rail control systems has resulted in an increasing reliance on digital technology and increased the potential for security breaches and cyber-attacks. This research paper showcases the need for developing the secure reusable scalable framework for enhancing cyber security of rail assets. A Cyber security framework has been proposed that is being developed to detect the tell-tale signs of cyber-attacks against industrial assets. This framework will be based on the concepts of developing protection profiles for railway assets such as point machine and evaluation assurance level in order to certify that chosen railway asset meet required security and safety properties. Endeavor is to make cyber health assessment of railway assets to prevent cyber-attacks.

6.2. Cyber Security Strategy September 2013", *Network Rail*, 2013, [online]. Available:https://www.networkrail.co.uk/WorkArea/DownloadAsset.aspx?id=30064788605.

Industrial Control Systems (ICS) were originally built on proprietary technology and primarily focused on "up-time" and "safety". Being isolated from the business environment they were independent islands of networked devices. However, ongoing advancements in business technology, brought with it new possibilities, such as the ability to access data and systems located inside of the previously isolated ICS environments. At this point many Industrial Control Systems (ICS) moved from proprietary technologies, to using the same protocols as business IT systems. This paradigm shift has led to an evolving convergence of business and process control networks, which has generated the effect of increased efficiency and visibility to field operations, but also brought with it new cyber security challenges.

Modern technologies contain well known cyber exploits and vulnerabilities which are now inherited in the ICS environment. As a result, ICS environments find themselves directly in the crosshairs of cyber attackers. Effective management of these cyber security challenges and exposures in the ICS environment has emerged as an important and dynamic element in the operational safety, security, and reliability of the infrastructure in the oil & gas industry.

6.3. M. Abrams, J. Weiss, "Malicious control system cyber- security attack case study-Maroochy Water Services" in , Australia. McLean, VA:The MITRE Corporation, 2008.

In this paper, we show that a malicious user can attack a large computing infrastructure by compromising the environmental control systems in the facilities that host the compute nodes. Such violations cannot be easily recognized by the administrators who manage the cluster, because of limited observation of the events in the cyber-physical systems. We describe real cases of failures due to problems in the cooling system of Blue Waters, the pet scale supercomputer of the University of Illinois at Urbana-Champaign. Blue Waters has cooling cabinets that use chilled water provided by the National Petascale Computing Facility (NPCF). We demonstrate, using real data, that the control systems that provide chilled water can be used as entry points by an attacker to indirectly compromise the computing functionality through the orchestration of clever alterations of sensing and control devices. In this way, the attacker does not leave any trace of his or her malicious activity on the nodes of the cluster. Failures of the cooling systems can trigger unrecoverable failure modes that can be recovered only after service interruption and manual intervention.

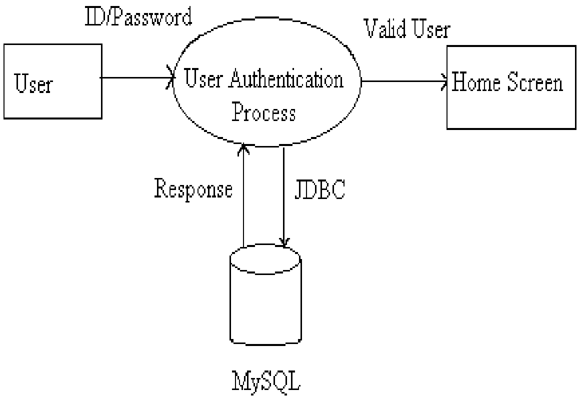
6.4. Dynamic Watermarking: Active Defense of Networked Cyber–Physical Systems Bharadwaj Satchidanandan; P. R. Kumar Proceedings of the IEEE

The coming decades may see the large scale deployment of networked cyber-physical systems to address global needs in areas such as energy, water, health care, and transportation. However, as recent events have shown, such systems are vulnerable to cyber attacks. Being safety critical, their disruption or misbehavior can cause economic losses or injuries and loss of life. It is therefore important to secure such networked cyber-physical systems against attacks. In the absence of credible security guarantees, there will be resistance to the proliferation of cyber-physical systems, which are much needed to meet global needs in critical infrastructures and services. This paper addresses the problem of secure control of networked cyber-physical systems. This problem is different from the problem of securing the communication network, since cyber-physical systems at their very essence need sensors and actuators that interface with the physical plant and malicious agents may tamper with sensors or actuators, as recent attacks have shown. We consider physical plants that are being controlled by multiple actuators and sensors communicating over a network, where some sensors could be “malicious,” meaning that they may not report the measurements those they observe. We address a general technique by which the actuators can detect the actions of malicious sensors in the system and disable closed-loop control based on their information. This technique, called “watermarking,” employs the technique of actuators injecting private excitation into the system, which will reveal malicious tampering with signals. We show how such an active defense can be used to secure networked systems of sensors and actuators.

7. Modules:

7.1 Login:

This module is taken into account only if there's a demand of safety and security by the client. solely once the login method, the remainder of the applying is created offered to the user. so as to login, user has got to 1st register by providing desired user-ID and word. Provided user-IDs and passwords by the users ar maintained during a info. Oracle info is employed to take care of a info. Then the user logins in to the applying by giving user-ID and word provided throughout registration method. JDBC is employed to attach the applying with the info.



7.2 Encryption of Field Data:

The actual field information is encrypted victimization AES algorithmic rule excepting Sensitive

7.3 Image Steganography of Data:

The Encrypted or Hashed information fields ar once more subject to image steganography severally.

7.4 Byte Array Conversion of Images:

Each Image that hides the particular field information needs to be regenerate into bytes for storage within the info.

7.5 Retrieval of Images:

It converts every field image computer memory unit array into image for de-embedding the particular information.

7.6 De-embedding knowledge from Images:

Each Image containing encrypted field knowledge is subject to de-embed method to urge the encrypted knowledge.

7.7 Decryption of knowledge fields:

Each knowledge field is decrypted to urge the particular knowledge to show on the web site once more.

7.8 Hash Comparison of Sensitive data:

It compares passwords or sensitive knowledge for login to a selected user.

7.9 Editing Module:

The data thus obtained is displayed for modification or deletion and change mistreatment crypto and steganographic techniques into the info once more.

8. Conclusion:

An approach that may just about defend the information from virtually associate degree sort of cyber attack on databases (For example: protection from an SQL Injection attack).Having delineate and illustrated the principles of the technology with relation to specific implementations, it'll be recognized that the technology may be enforced in several different, different, forms. To produce a comprehensive revelation while not unduly perpetuation the specification, candidates incorporate by reference the patents and patent applications documented on top of. The strategies, processes, and systems delineate on top of is also enforced in hardware, code or a mix of hardware and code. As an example, the auxiliary knowledge secret writing processes is also enforced in a very programmable laptop or a special purpose digital circuit. Similarly, auxiliary knowledge cryptography is also enforced in code, firmware, hardware, or mixtures of code, code and hardware. The strategies and processes delineate on top of is also enforced in programs dead from a system's memory (a machine readable medium, like associate degree electronic, optical or magnetic medium device). The particular mixtures of parts and options within the above-detailed embodiments are exemplary only; the interchanging and substitution of those teachings with different teachings during this and also the incorporated-by-reference patents/applications also are contemplated. The Databases ar therefore to be secured victimization secure steganographic techniques to hide text within pictures and store these pictures as blobs within the tables created within these databases to form the databases strong and resistant to SQL Injection Attacks.

9. Future Scope:

The projected approach during this project uses a steganography approach known as image steganography. The appliance creates a steganography image during which the non-public knowledge is embedded and is protected with a watchword which is extremely secured. The most intention of the project is to develop a steganography application that has sensible security. The projected approach provides higher security and might shield the message from steganography attacks. The image resolution does not amendment abundant and is negligible once we engraft the message into the image and also the image is protected with the non-public watchword. So, it's unacceptable to break the info by unauthorized personnel. We are going to use the smallest amount important Bit formula during this project for developing the appliance that is quicker and reliable and compression magnitude relation is moderate compared to alternative algorithms.

The major limitation of the appliance is meant for bit map pictures (.bmp). It accepts solely bit map pictures as a carrier file, and also the compression depends on the document size in addition because the carrier image size. The long run work on this project is to boost the compression magnitude relation. The safety victimization least important Bit formula is sweet however we will improve the amount to an exact extent by variable the carriers in addition as victimization totally different keys for cryptography and decipherment.

10. References:

[1]. Java Complete Reference by Herbert Shield

[2]. Database Programming with JDBC and Java by George Reese

[3]. Java and XML By Brett McLaughlin

[4]. G. Aggarwal, T. Feder, K. Kenthapadi, S. Khuller, R. Panigrahy, D.Thomas, and A. Zhu, "Achieving Anonymity via Clustering,"Proc. 25th ACM SIGMOD-SIGACT-SIGART Symp. Principles of Database Systems (PODS).

[5]. R. Agrawal, P.J. Haas, and J. Kiernan, "Watermarking Relational Data: Framework, Algorithms and Analysis," The Int'l J. Very Large Data Bases, vol. 12.

[6]. V. Athitsos, M. Potamias, P. Papapetrou, and G. Kollios, "Nearest Neighbor Retrieval Using Distance-Based Hashing," Proc. IEEE24th Int'l Conf. Data Eng. (ICDE).

[7]. Java Servlet programming by O'Relly publishers.