**Project Synopsis**

**Content**

* **Title of the Project**
* **Introduction and Objectives of the Project**
* **Project Category**
* **Research Methodology**
* **Scope of the solution**
* **Analysis**
* **Future scope and further enhancement of the project**
* **Bibliography and Literature survey**

|  |
| --- |
| **Title of the Project** |

“Security analysis and security implementation on Inventory management web application & case study on related cyber crimes”.

|  |
| --- |
| **Introduction and Objectives of the Project** |

**Purpose**

The main purpose of this project is to focus on real life application scenario in terms of information security. The agenda would be to build an application and implement the security by identifying the “security loop holes” and analysis on cyber crimes.

The reason behind taking this project is to combine the theoretical knowledge and practical knowledge of real life scenario.

**Objectives**

Security is not just limited to data and resources, the coding should be done by considering vulnerabilities.

The project is divided into two portions. First part emphasizes on analysis and implementation of information security in application and the second part is the case study of cyber crimes in India related to same.

Information security is very important in an organization to protect the applications that implemented in organizations. We need security to reduce the risk of unauthorized information disclosure modification and destruction.

There are several challenges in our constantly changing environment that makes it difficult to adequately protect our resources. There are blending the corporate and personal live, inconsistent enforcement of policies, lack of awareness in information security, information security threat.

The purpose of this Supermarket Inventory System is to facilitate our customers to track their products as and when they are transported from the vendor to the warehouse and from the warehouse to the retail location to the customers.

It also aims to acquaint the user with the position of the supermarket currently by producing various sale graphs of items based on what quantity of a certain item is sold on a daily, weekly, monthly and yearly basis.

The Inventory Management System is an application designed to allow the supermarket staff to create, maintain and view the contents and value of its inventory of items in a categorized way.

## It also aims to analyze the position of the supermarket in the market and help it know what items to order in what quantity by producing graphs depicting sale of different items on different basis such as monthly, yearly, brand type etc.

**Goal**

## It is necessary to keep our resources safe and protected. In order to implement security in application it would be done by implementing encryption, keeping secure session base password, implementing two level authentications, observing system logs and security faults, analyzing network flow using wireshark, implementing wireshark, preventing the application validation from un-necessary inputs, and implementing code to prevent from SQL injection.

## Every crime has its impact specifically on society, nation and the world to the great extent. To understand the influence of cybercrime, it is necessary to look into the impact of two things computer technology and internet on people as cybercrime is no doubt originating out of these.

## This project also includes the study on Cyber Crime cases in India and suggestions on how to minimize its vulnerability. I am also planning to prepare a research term paper on same.

**Tools used to implement application and security**

1. **HTML-PHP**

PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language. PHP code can be simply mixed with HTML code, or it can be used in combination with various template engines and web frameworks. PHP code is usually processed by a PHP interpreter, which is usually implemented as a web server's native module or a Common Gateway Interface (CGI) executable.

1. **JavaScript**

JavaScript, often abbreviated as JS, is a high-level, dynamic, weakly typed, prototype-based, multi-paradigm, and interpreted programming language. Alongside HTML and CSS, JavaScript is one of the three core technologies of World Wide Web content production. It is used to make webpages interactive and provide online programs, including video games.

The majority of websites employ it, and all modern web browsers support it without the need for plug-ins by means of a built-in JavaScript engine.

1. **CSS**

Cascading Style Sheets (CSS) is a simple mechanism for adding style (e.g., fonts, colors, spacing) to Web documents. These pages contain information on how to learn and use CSS and on available software. They also contain news from the CSS working group.

1. **Web server – WAMP**

WAMP is an acronym for an archetypal model of web service solution stacks, originally consisting of largely interchangeable components: Windows, the Apache HTTP Server, the MySQL relational database management system, and the PHP programming language. As a solution stack, LAMP is suitable for building dynamic web sites and web applications.

1. **Development tool – RAD**

Rapid Application Development Software lifecycle

1. **Database platform – MySQL**

MySQL the world's second most widely used open-source Relational Database Management System (RDBMS).

1. **Network security platform – WireShark**

WireShark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

1. **Application security – Encryption and Decryption**

In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it.

Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating ciphertext that can only be read if decrypted.

For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

1. **Application security – Validation**

Data validation is the process of ensuring that user input is clean, correct, and useful.

Most often, the purpose of data validation is to ensure correct user input. Validation can be defined by many different methods, and deployed in many different ways.

Server side validation is performed by a web server, after input has been sent to the server.

Client side validation is performed by a web browser, before input is sent to a web server.

It Helps Cross-Browser, Cross-Platform and Future Compatibility

Although you may be able to create a web page that appears to work on your favorite browser (whatever that may be), your page may contain HTML or CSS errors that do not show up with that browser due to an existing quirk or bug. Another person using a different browser that does not share that particular bug will end up viewing a page that does not show up correctly. It is also possible that later versions of your browser will fix that bug, and your page will be broken when people use its latest incarnation.

Coding your pages so that it is correct without errors will result in pages that are more likely to work across browsers and platforms (ie, different systems). It is also a form of insurance against future versions of browsers, since all browsers aim towards compliance with the existing HTML and CSS standards.

1. **Search Engine Visibility**

When there are errors in a web page, browsers typically try to compensate in different ways. Some may ignore the broken elements while others make assumptions about what the web designer was trying to achieve. The problem is that when search engines obtain your page and try to parse them for keywords, they will also have to make certain decisions about what to do with the errors. Like browsers, different search engines will probably make different decisions about those errors, resulting in certain parts of your web page (or perhaps even the entire page) not being indexed.

The safest way to make sure the search engines see the page you want them to see is to present them an error-free page. That way, there is no dispute about which part of your page comprises the content and which the formatting code.

1. **System security logs – Fiddler**

Fiddler is an HTTP debugging proxy server application written by Eric Lawrence, formerly a Program Manager on the Internet Explorer development team at Microsoft.

Fiddler captures HTTP and HTTPS traffic and logs it for the user to review (the latter by implementing man-in-the-middle interception using self-signed certificates).

Fiddler can also be used to modify ("fiddle with") HTTP traffic for troubleshooting purposes as it is being sent or received. By default, traffic from Microsoft's WinINET HTTP(S) stack is automatically directed to the proxy at runtime, but any browser or Web application (and most mobile devices) can be configured to route its traffic through Fiddler.

1. **Case Study on Cyber Crimes in India on online applications**

Computer crime is a general term that embraces such crimes as phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, kidnapping children via chat rooms, scams, cyber terrorism, creation and distribution of viruses, spam and so on.

The advancement of technology has made man dependent on Internet for all his needs. Internet has given man easy access to everything while sitting at one place. Social networking, online shopping, storing data, gaming, online studying, online jobs, every possible thing that man can think of can be done through the medium of internet. Internet is used in almost every sphere. With the development of the internet and its related benefits also developed the concept of cyber crimes.

Cyber crimes are committed in different forms. A few years back, there was lack of awareness about the crimes that could be committed through internet. In the matters of cyber crimes, India is also not far behind the other countries where the rate of incidence of cyber crimes is also increasing day by day.

It is not just limited to that; it can be applied on online websites, portals and net banking too.

Attackers are always trying to hack the resources which demand the high value. Nowadays net banking is very crucial. People easily get wrapped into spam and become phishing target due to lack of awareness about security.

This chapter will emphasize on such scenarios that happened in India and what kind of actions took by government, we will try to suggest the workaround to how we can reduce it vulnerabilities.

This case analysis is important in this project as it is about web application, to create awareness about “Web Hijacking”.

Web hijacking means taking forceful control of another person’s website. In this case the owner of the website loses control over his website and its content.

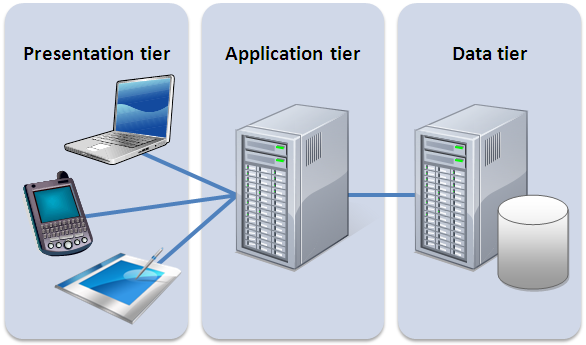
|  |
| --- |
| **Project Category** |

This project is covering the skills and core areas of Information Security with equal emphasis on the theory and practice. The main focus is to implement an application and analyze security issues in the applications followed by case study on cyber crimes in India in the same area.

**Application Architecture**

Three tier architecture

Three-tier architecture is a client–server software architecture pattern in which the user interface(presentation), functional process logic ("business rules"), computer data storage and data access are developed and maintained as independent modules, most often on separate platforms.



The three tiers in three-tier architecture are:

1. Presentation Tier: Occupies the top level and displays information related to services available on a website. This tier communicates with other tiers by sending results to the browser and other tiers in the network.
2. Application Tier: Also called the middle tier, logic tier, business logic or logic tier, this tier is pulled from the presentation tier. It controls application functionality by performing detailed processing.
3. Data Tier: Houses database servers where information is stored and retrieved. Data in this tier is kept independent of application servers or business logic.

|  |
| --- |
| **Research Methodology** |

**Rational Unified Process**

This software engineering process has three branches from all of the generic process models that a standard software engineering project would requires or is entitled to, it also supports regular revisions and it also provides guidelines of “standard practices” in system analysis and design.

This model is best described by following three perspectives:

**Static |** This phase shows the set of actions that are carried out over development period

**Dynamic |** This phase shows an overview of phases that covers major aspects of development

**Practice |** These phases are guidelines that provides the bases of standards that should be followed



**Methodology**

**Inception** | The objective of this phase is to provide the outline to the organization for the system. This includes identification of all the factors and entities that will be the part of communication system either to the system or from the system. Collection of this information will help create the business case for the proposed system.

**Elaboration** | This phase mainly encloses the entities related to the bases of understanding the problem, its domain, the framework of architecture and the project plan and most importantly the stakeholder and risk associated with each of them.

**Construction** | Although previous phase may include the activities related to establishing the grounding framework of this project, this phase is actually dedicated to the overall system design, implementation and testing. Parts of the system may be developed in small sized units and finally are coupled together during this phase.

**Transition** | This last phase is concerned with deploying the system to the customer base from the testing and development environment.

**Literature survey**

There might be many existing system but there is lack of security. We are trying to build efficient system with security implementation and how to keep application safe and secure by preventing web attacks. It also includes the analysis how application can be hacked and how to prevent it. This will contain case study on cyber crimes in India related to the same.

**Analysis on how cyber stalkers operate to hack website**

They collect all personal information about the victim such as name, family background, Telephone Numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc. If the stalker is one of the acquaintances of the victim he can easily get this information. If stalker is a stranger to victim, he collects the information from the internet resources such as various profiles, the victim may have filled in while opening the chat or e-mail account or while signing an account with some website.

Some stalkers keep on sending repeated e-mails asking for various kinds of favors or threaten the victim.

In online stalking the stalker can make third party to harass the victim.

1. **DDoS**

Denial of Service is an attack in which the criminal floods the bandwidth of the victim’s network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide. This kind of attack is designed to bring the network to crash by flooding it with useless traffic. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCp/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by Hacker.

1. **Viruses**

Viruses are the programs that have the capability to infect other programs and make copies of itself and spread into other program. Programs that multiply like viruses but spread from computer to computer are called as worms. These are malicious software that attach themselves to other software. Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious. Viruses usually affect the data on a computer, either by altering or deleting it. On the other hand worms merely make functional copies of themselves and do this repeatedly till they eat up all the available.

1. **Software piracy**

Software piracy refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. These kind of crimes also include copyright infringement, trademarks violations, theft of computer source code, patent violations etc.

**Analysis on how to prevent application from hacking**

**1. Keep software up to date**

This applies to both the server operating system and any software you may be running on your website.

**2. Implement PHP code to prevent SQL Injection**

SQL injection attacks are when an attacker uses a web form field or URL parameter to gain access to or manipulate your database. When you use standard Transact SQL it is easy to unknowingly insert rogue code into your query that could be used to change tables, get information and delete data. We can easily prevent this by always using parameterized queries, most web languages have this feature and it is easy to implement.

"SELECT \* FROM table WHERE column = '" + parameter + "';"

If an attacker changed the URL parameter to pass in ' or '1'='1 this will cause the query to look like this:

"SELECT \* FROM table WHERE column = '' OR '1'='1';"

Since '1' is equal to '1' this will allow the attacker to add an additional query to the end of the SQL statement which will also be executed.

We could fix this query by explicitly parameterising it. For example, if we're using MySQLi in PHP this should become:

$stmt = $pdo->prepare('SELECT \* FROM table WHERE column = :value');

$stmt->execute(array('value' => $parameter));

**3. Error messages**

We need to be careful with how much information you give away in our error messages. Provide only minimal errors to our users, to ensure they don't leak secrets present on our server (e.g. API keys or database passwords). Don't provide full exception details either, as these can make complex attacks like SQL injection far easier. Keep detailed errors in our server logs, and show users only the information they need.

**4. Server side validation/form validation**

Validation should always be done both on the browser and server side. The browser can catch simple failures like mandatory fields that are empty and when you enter text into a numbers only field. These can however be bypassed, and we should make sure we check for these validation and deeper validation server side as failing to do so could lead to malicious code or scripting code being inserted into the database or could cause undesirable results in our website.

**5. Passwords**

Passwords should always be stored as encrypted values, preferably using a one way hashing algorithm such as SHA. Using this method means when we are authenticating users we are only ever comparing encrypted values. For extra website security it is a good idea to salt the passwords, using a new salt per password.

Everyone knows they should use complex passwords, but that doesn’t mean they always do. It is crucial to use strong passwords to your server and website admin area, but equally also important to insist on good password practices for our users to protect the security of their accounts.

In the event of someone hacking in and stealing our passwords, using hashed passwords could help damage limitation, as decrypting them is not possible. The best someone can do is a dictionary attack or brute force attack, essentially guessing every combination until it finds a match. When using salted passwords the process of cracking a large number of passwords is even slower as every guess has to be hashed separately for every salt + password which is computationally very expensive.

**6. File uploads**

Allowing users to upload files to our website can be a big website security risk, even if it’s simply to change their avatar. The risk is that any file uploaded however innocent it may look, could contain a script that when executed on our server completely opens up our website.

No not allow file uploads.

**7. HTTPS**

HTTPS is a protocol used to provide security over the Internet. HTTPS guarantees to users that they're talking to the server they expect, and that nobody else can intercept or change the content they're seeing in transit.

If we have anything that our users might want private, it's highly advisable to use only HTTPS to deliver it. That of course means credit card and login pages (and the URLs they submit to) but typically far more of our site too. A login form will often set a cookie for example, which is sent with every other request to our site that a logged in user makes, and is used to authenticate those requests. An attacker stealing this would be able to perfectly imitate a user and take over their login session. To defeat these kinds of attacks, we almost always want to use HTTPS for our entire site.

**8. Website security tools**

Once we think we have done all we can then it's time to test our website security. The most effective way of doing this is via the use of some website security tools, often referred to as penetration testing or pen testing for short.

**9. Two Level authentication**

Passwords play an important role in daily life in various computing applications and play a critical role in online authentication. The main aim for using passwords is to restrict unauthorized users to access the system.

Passwords are necessary to provide the security to the users because of many flaws in the conventional password systems. Unfortunately, passwords suffer from two intractable problems: password cracking and password theft. So we use Password hashing to protect password. Password hashing technique allows users to remember simple passwords and have them hashed to create secure passwords. This paper describes widely used hash algorithms and comparative analysis of different hash algorithms which are used in password hashing for making awareness of attacks and selection of hashing method in a particular scenario.

In current scenario, where the number of internet users is widely increasing, internet has become the primary medium of communication. So, user’s data attains the greatest priority in the field of data communication. To keep the network usage reliable, data integrity, data authentication, non-repudiation, data confidentiality is of utmost importance.

Password is one of the most common security method to authenticate user’s identity in online. They provide a powerful guard against unauthorized access to systems and data. Password occupy the important position in user authentication because other authentication factors something you have and something you are (e.g. Fingerprint) not gained a wide on the Internet, primarily because of their limited flexibility, high cost and restricted portability.

On the other side, passwords are simple, easy to implement and inexpensive. Despite their prevalence Password Hashing security depend passwords on protecting passwords from being stolen. A strong password should be sufficiently long, random, and hard to discover by crackers. However, no matter how strong they are, passwords are also vulnerable to theft like phishing and shoulder surfing.

A technique to obtain secure online passwords is password hashing, where hashed passwords are sent to databases or remote websites. Hashing is an important technique used for secure communication in the presence of eavesdroppers. It provides all the paramount aspects of information security such as integrity, authentication and confidentiality.

Password hashing is lightweight and convenient to use and can defend against phishing attacks.

We will implement the two level authentications to provide the high level security in an application.

|  |
| --- |
| **Scope of the solution** |

This Supermarket Inventory System creates purchase orders once the inventory level reaches to a pre-defined level. Supermarkets and the vendor’s warehouse use this system to create receipt and invoice. The accounting department uses this system to match invoice and receipt so that the payment can be recorded accurately.

By this project we will be able to focus on both small and big retail stores in helping manage their Inventory of their store with security implementation. If taken in more general form it can be used to manage inventory of even Production House’s and Warehouse’s.

The Inventory Management System is an application designed to allow the supermarket staff to create, maintain and view the contents and value of its inventory of items in a categorized way.

It also aims to analyze the position of the supermarket in the market and help it know what items to order in what quantity by producing graphs depicting sale of different items on different basis such as monthly, yearly, brand type etc.

The main goal as of now is to implement application by considering security loop holes. We will analyze and implement web security in this project followed by case study on cyber crimes in India.

By security inputs, it will decrease the vulnerability of application being from hacked and attacks. It provides the surety and trust to the customers that their resources are safe and secure. Customers trust should be an organizations job.

It also determines the use of information security at its pick level to resolve the real world problems.

|  |
| --- |
| **Analysis** |

The project analysis will be based upon below three concepts.

Data held on IT systems is valuable and critical to the business of the University. We all rely on IT to store and process information, so it is essential that we maintain Information Security.

The analysis of information security policies is to preserve:

**Confidentiality** | Data is only accessed by those with the right to view the data.

**Integrity** | Data can be relied upon to be accurate and processed correctly.

**Availability** | Data can be accessed when needed.

Failure to comply with the requirements of these Information Security Guidelines may lead to disciplinary action.

|  |
| --- |
| **Future scope and further enhancement of the project** |

Information security is crucial in organization. All information stored in the organization should be kept secure. Information security will be defined as the protection of data from any threats of virus.

The information security in important in the organization because it can protect the confidential information, enables the organization function, also enables the safe operation of application implemented on the organization’s Information Technology system, and information is an asset for an organization.

Even though the information is important in organization, there are several challenges to protect and manages the information as well. One of challenges faced in an organization is the lack of understanding on important of information security.

When employees is lack of information security knowledge in term of keeping their information, the organization is easy to being attacks by hackers or another threats that try to stole or get the organization confidential information. So it is crucial and important to all staff in an organization to have knowledge and understanding about the importance information security practice in an organization to protect the confidential data.

Future scope of this project is vast, as we are trying to implement security and decreasing loop holes that help to create security awareness.

It will be helpful and used in government organizations, private companies, non private sectors; researchers to make it much better and would be refer by institutions too.

Further enhancement of this project will really help to build own company that provides Inventory support with all security features that will be used by all store keepers, allow the supermarket staff to create, maintain and view the contents and value of its inventory of items in a categorized way with less vulnerability. This system is a tool for tracking asset levels, order management, safety stock, sales and deliveries. It would help to avoid product overstock and outages.

System that contains a list of orders to be received and then prompts workers to pick the necessary items, and provides them with packaging and shipping.

|  |
| --- |
| **Bibliography and Literature survey** |

The software requires a connection to a database server containing the inventory database. The program will be executed as a standalone application on a single machine. The application may be executed on multiple machines simultaneously. The user will interact with the program via a GUI. The user will use both the mouse and keyboard for input and all information will be outputted to the monitor.

**Problem Statement**

|  |  |
| --- | --- |
| The problem of | Inventory management in supermarkets |
| Affects | Customers, Manufacturers, Retailers |
| The impact of which is | Overstock, Outages, ignorance of profitable goods |
| A successful solution would be to | Design of a database for storing the entire inventory, a front end for user interaction with the system, and analysis of daily, weekly, monthly or yearly sales on different types and brands with implementation of validation, encryption, session two level authentications, with WireShark and Fiddler security analyzer tools. |

**Product Positioning System**

|  |  |
| --- | --- |
| For | Manager, store-keeper and owner |
| The (product name) | Inventory Management System |
| That | Avoids tedious hand-keeping format for storing various information and provides efficient, user-friendly computer base management system with highly security mechanisms that ensures the data protection |

**User Summary**

|  |  |  |
| --- | --- | --- |
| **Name** | **Description** | **Stakeholder** |
| Owner  Manager  Store Keeper | To keep check on the whole working of the super market (both market and inventory).  To keep track record and market analysis of the entire inventory.  To keep track record of the currently available quantity. |  |

**User Environment**

The total number of user depends on the employee given authority to check the inventory.  
The time required to check the inventory using system is less than a minute.  
The system setup is purely in-door and can be used remotely if internet facility is use with high level security.

**Literature survey**

1. **Study of different software development lifecycle model**

* The linear sequential model
* The prototype model
* The RAD model
* Evolutionary software process
* The incremental model
* The spiral model

1. **Study on inventory system**

* Study on real time issues on retailers store and supermarkets
* Analysis on overstock, outages, ignorance of profitable goods
* Affects on Customers, Manufacturers, Retailers

1. **Study of information security concepts**

* Unauthorized Access and Hacking
* Web Hijacking
* Cyber Stalking
* Denial of service Attack
* Virus attacks
* Software Piracy
* Salami attacks
* Phishing
* Sale of illegal articles
* Online gambling
* Email spoofing
* Cyber Defamation
* Forgery
* Theft of information contained in electronic form
* Email bombing
* Data diddling
* Internet time theft
* Physically damaging a computer system
* Theft of computer system
* Breach of Privacy and Confidentiality
* E-commerce/ Investment Frauds

1. **Comparison of different Encryption algorithms**

* Basics of Encryption
* Ciphers
* History
* Importance
* Types of Cryptography
* Importance of Encryption
* AES Algorithm
* Symmetric key DES
* Asymmetric key RSA
* Algorithm comparison criteria
* Comparison between DES and RSA
* Hash function MD2 Algorithm
* Hash function MD4 Algorithm
* Hash function MD5 Algorithm
* Hash function SHA1 Algorithm
* Hash function Crypt Algorithm
* Cryptanalytic attacks

1. **Study of WireShark**

* Security analysis of non trusted sites using WireShark
* Security analysis of trusted sites using WireShark

1. **Study of Fiddler**

* Study of HTTP debugging proxy server
* Analysis on HTTP/HTTPS traffic

1. **Study on Application Validation**

* Session management
* Password validation with respect to AIEEE standards
* Customer validation
* Server side validation and Client side validation

1. **Study on how to prevent application from being hacked**

* Study on secure coding using SQL-Injection
* Session based password protection
* Two level authentications
* Analysis on TSL/SSL secure certificate web applications

1. **Study of vulnerability of application being hacked**

* DDoS
* Viruses
* Software piracy

**Bibliography**

Web references:

1. [www.google.com](http://www.google.com)
2. [www.wikipedia.com](http://www.wikipedia.com)
3. <http://cyberlawsindia.net>
4. <https://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/>
5. <http://www.cyberralegalservices.com>
6. <https://www.tradegecko.com>
7. <https://www.cdse.edu/resources/case-studies/information-security.html>
8. <https://www.ibm.com/security/solutions/>

Articles:

1. Supply Chain Inventory Management and the Value of Shared Information by Gerard P. Cachon and Marshall Fisher.
2. Exploring the knowledge inventory in project-based organizations: a case study by Dirk Pieter van Donk and Jan Riezebos
3. Introduction to materials management by JRT Arnold, SN Chapman and CM Clive.
4. Operations management by WJ Stevenson and M Hojati.
5. Computer security: principles and practice by W Stallings, L Brown, MD Bauer and AK Bhattacharjee.
6. Integrating case study and survey research methods: an example in information systems by European journal of information systems.
7. ISRAM: information security risk analysis method by B Karabacak.
8. The positive outcomes of information security awareness training in companies–A case study by M Eminagaoglu, E Ucar and E Eren.
9. Network Security: A Case Study by SJ Lincke.

|  |
| --- |
| **Declaration** |

I hereby declare that the above provided information is true and best of my knowledge. My plan is to complete the proposed system as part of program post graduate diploma in information security. The project title was finalized as per the guidelines and instructions provided by program coordinator, IGNOU, Delhi. The reason to take this project was to focus on implementation with security concepts. I will try to research more on cyber crimes too and will build a research term paper. The first part would be to implement the security in real life project and second part is to prepare the term paper on cyber crimes in India on the same. The project includes sufficient work considering timeframe.

**Thanks and Regards,**

**Yamini Rathod**