Chapter 2 LITERATURE REVIEW

1. **Ganesan R. (2010)**
The author, writes about what are the cyber trends for 2010-11. The author defines “drive-by download” such as Malware, Worms, and Trojan horses. The author says that Botnets and zombies will continue to proliferate. The author introduces a term “Scareware” - Scareware is fake/rogue security software. Be cautious about all communications; do not open attachments from un-trusted sources.

2. **Balasubramanian S. – Honeywell (2010)**
The author says that one of the key inhibitors for organizations to adopt Cloud Computing practices is the perceived risks around information security. As Cloud Computing requires organizations to source their IT needs outside of their corporate network, the traditional enterprise security practices are being challenged & it demands alternate security models. This paper describes the security risks identified in the Cloud Environment and the solution offered by Jericho security model to address these risks.

A group of authors from "wipro council for industry research" discussed about the security in the information age: the rise of cyber attacks the threat of a new age of cyber threats, cyber wars, and cyber espionage are on the rise, and with this, a whole new dimension arises in the realms of cyber security. A combination of technical expertise, law and an effective security infrastructure are the need of the hour towards achieving the objective of securing the information assets of the country.

The author discussed the Dilemma and possible solutions. North Korean hackers may have stolen secret defense plans, The author claims that The US is a leading source of who use digital tools to attack government websites, computer systems and censorship tools in Iran and China. According to the author A comprehensive approach involving all sectors -- government, industry, business and academia - is essential.

The author puts forward his point that the weak link in cyber safety - the human angle. He points out that the place of the crime, the criminal and the machinery used can be out of the Indian jurisdiction. Today Internet is used by common people, making them easy targets for cyber criminals. Data is a broad categorisation, from credit-card information to bank and other financial records to personal information. The current resolution to this very grave and far-reaching issue lies in basic awareness, protection and care, by education.

The author discusses Cyber Threats & Challenges in Real World. Cyber threats are not limited to cyber world alone. The real threat in this networked world which is increasingly becoming automated, where it is possible to take control of and manipulate the process control systems critical infrastructure is a living nightmare. To derive real advantage of these automation requires all these instruments and processes to be networked. We need to create authorized secure environments for the entry of data and analysis of the processes.

8. Mugil, Raja, Mathiyazhagan, Chandrasekar (2010)
The authors, emphasis the importance of Internet Security. Instant Messaging is popular with businesses and individuals, a business email intercepted during its transmission may let slip business confidentiality; file transfers via instant messengers may also be intercepted, ID and password theft may lose us money when using Internet bank service. Type the URL directly. (2) Online banking certifications are currently the most effective security safeguard measure. (3) Do not trust e-mails that ask for your account number and passwords.

The author discusses basic issues of Data Protection System (DPS). He highlights the “outsourcing menace”. The author emphasis on the need of updating of technology at all levels of their assets but also their psychological comfort and faith in the e-system. Author suggests a few “acid-tests” for system management. OTP (One Time Password), “multiband” authentication, Data Loss prevention are the key words.

The author quotes Ethan Katsh- "... Where there are significant challenges to the legal profession and to the traditional legal practices and concepts. To an unfamiliar and rapidly changing information environment ...” To summarise the dilemma surrounding the internet. All have witnessed cyber attacks that they are still coping with attempts to counteract and to prevent continued assault. New techniques for monitoring, tracking, and trapping criminals have been developed. The need is to formulate a rationalized, global cybercrime law that can be understood across borders.

The Author points out an technology is playing an important role not only in fraud perpetration but also in fraud detection. While fraudsters take advantage of technology to perpetrate crime, companies can use technology intelligently to mitigate fraud risks. Data mining and data analysis
are techniques that are fast playing a key role in fraud detection and mitigation efforts. He discusses the pros and cons of this methodology. Such as: Lack of skilled resources, ability to evaluate full transaction, continuous evolving “known” fraud scenarios, “False-positives”.

The author, discusses how Data mining techniques and tools are useful in the process Cyber investigation. The challenge lies in finding and preserving useful data and presenting it in a manner acceptable in a court of law. Text data mining and Image Video data mining technologies will provide solutions in future to help the intelligence and Investigation experts by giving relevant, useful hidden knowledge from the huge digital data of the cyber world.

The author discusses the colossal change in the pattern in which conventional wars are being conducted. The Author will also shatter the conventional wisdom on cyber defence which relies on the notions of "layers of defences" and Legal instrument, by providing a new approach to cyber defence The Author believes that this framework will raise information warfare to the strategic level which it duly deserves.

The author addresses the present day cyber threats; security solutions that are required address them. It does not have any limitation of use and can achieve most of the goal set. Hence, providing multi layer security protects information shared in a networked environment of military communication. ICT drives the operations of communication in commercial to achieve information security; migration to multi layer security is need of the hour.

The author says that Cyberwarfare is not, as many people think, limited to government attacking government; any part of the critical infrastructure may be subject to attack, from banking and telephone companies to transport or the supply of essential goods and commodities. A sound e-governance policy presupposes the existence of a sound and secure e-governance base as well. The security and safety of various ICT platforms and projects in India must be considered on a priority basis before any e-governance base is made fully functional.

The author, Information Technology Advisor, in his article, “security convergence - physical and information” compares between Physical and Information Security. Security convergence refers to the convergence of two physical security. Security convergence is motivated by the recognition that corporate assets are increasingly information-based. Technology has transformed traditional business and facilitated the creation of entirely new ones by integrating technology into processes. With this, line between information security & traditional physical security have blurred.

17. Prof. Selvakani, Maheshwari V. & Karavanasundari (2010)
The Head and a group of students, say that the I.T. can be used for destructive as well as
constructive work. The authors believe that a computer can be secured even by a person with simple technical knowledge the ascertainment and preservation of the evidence is a tough task. There is need to secure the ICT infrastructures used for meeting these social functions. We need a techno-legal "harmonized law". A good combination of law and technology must be established.

A group of officers from Standard Chartered Bank, point out that with a high dependency on computers, neglecting the increase in Cyber crime is extremely dangerous. Hackers can misuse your personal information entry of virus into your system, altering your files. With every patch released for a particular weakness, being followed by the next exploit at the very next moment, one can never be sure that our systems are in safe hands. Business demands for new ways of technology WILL CONTINUE. Cyber Attacks WILL CONTINUE and hence Cyber Security SHOULD REMAIN A PRIORITY.

The Chairman, Cyber Society of India, Chennai, in his article discusses “Various Perceptive of Cyber Security”. Continuously evolving new threats against enterprise, IT have made cyber security a 'must look-into' important issue. The Systems Administration team should devise ways to Improve their cyber security with an automated, on-demand, application security testing solution that makes comprehensive cyber security for applications simpler and more cost-effective. Cyber security knows no borders. The author touches upon controlling server sprawl to increase operational efficiency and ease disaster recovery, virtualization clearly delivers bottom-line results.

This paper presents a comprehensive open source assessment of China's capability to conduct Computer Network Operations (CNO). The result will hopefully serve as useful reference to policymakers, China specialists, and information operations professionals. The research encompassed five broad categories to show how the People's Republic of China (PRC) is pursuing Computer Network Operations (CNO) and the extent to which it is implemented. The focus is providing the force for the development of an advanced Irregular Warfare (IW) capability. chief strategies driving the process of informatization in the PLA is the coordinated use of CNO, Electronic Warfare (EW).

A group of authors say Nuclear Power Plants have a lot of critical data to be sent to the operator workstations. A plant wide integrated communication network, with high throughput, determinism and redundancy, is required between the workstations and the field. Switched Ethernet network is a promising prospect for such an integrated communication network. In Nuclear Power Plants, the plant data is crucial & data loss cannot be tolerated, Switched Ethernet shall be an appropriate technology.
A pair of professors, states that Phishing scams pose a serious threat to end users. Email continues to be the favorite vehicle to perpetrate such scams. Several approaches have been proposed to address this problem. However, phishing techniques, growing in ingenuity & sophistication, render these solutions weak. In this paper the author propose a novel approach to detect phishing attacks using fake responses which mimic real users, essentially, reversing the role of the victim and the adversary.

A group of faculty say that Email is being abused by criminal community for various illegitimate purposes, such as E-mail spamming, drug-trafficking, cyber-bullying, phishing, racial vilification, child pornography, and sexual harassment etc. E-mail system security lacks adequate proactive mechanism, to defend against such vulnerabilities. They also proposed the implementation of a framework employing data mining and machine learning techniques for e-mail forensic analysis.

Authors from have recently expressed the need to mediate access to valuable database. This paper presents a forensic analysis algorithm which can help to determine when the tampering done and what is the affected region of database and also this algorithm is more efficient than prior algorithms as it introduces notion of candidate set. This algorithm employs a logarithmic number of hash chains within each tile to narrow down the when and what.

The authors present “S-box Modification in DES”. DES is Data Encryption Standards and S-box “substitution box” - a standard encryption device. Security is the main concern for organizations participating in information exchange. One essential aspect for secure communications is that of cryptography. As cyber crimes are causing serious financial losses, existing system needs constant modifications in order not to compromise with the security levels. It shows higher degree of resistance against attack on relationship \( L_{i+1} = R_j \). But a significant amount of mathematical knowledge and understanding the complete cryptosystem is required.

The authors, discuss that: accelerating customer demand, increased competition among banks themselves. The Zi with value less than one will be identified category of low awareness level of new internet banking users. If value is found greater than one then of high awareness level and if value equals one then new user will be identified as having medium level of awareness. Internet banking service providers can formulate different mix of promotional strategies for wider and effective acceptability of their products.

PG research group, says Phishing attacks have been growing rapidly and social aspect at the personal as well as industry altitude. Phishing has primary four different types of impacts: economic loss, lack of confidence on Internet, difficulties in fraud investigation. The paper
discusses the effectiveness of various anti-Phishing toolbars against phishing attack. The study showed that they are good in case of well known phishing web site. Proposed approach "Anti-Phishing design using mutual authentication" is good in the case of financial organization.

28. R. Chouhan, V. Singh Rathore (2011)
The authors, say banks are using the Internet as a new distribution channel. Standardization, Regulatory and Legal Issues, Infrastructure, Heavy Investment Costs, and Socio-Cultural Challenges amongst are the serious issues which had affected the development and security of the services as expected. The future of e-banking will be a system where users are able to interact with their banks "worry-free" and banks are operated under one common standard.

Faculty have made an exploratory study. Internet offers both informative as well as transactional mediums. Substantial number of peoples is using Internet not only for updating their knowledge with the latest information, but also for making purchase online. The study is based on the primary data collected from the sample of 164 respondents drawn from service class Internet users located in Indore city. The outcome of the study would be helpful to the marketers in the development of strategies for increasing online sales.

Faculty members talk about the study of Obstacles in Cloud Computing. Cloud Computing is becoming a well-known buzzword nowadays. Many organizations are accelerating their paces in developing Cloud Computing systems and enhancing their services. The obstacles presented in terms of availability of service, Data Lock-In, Data Confidentiality and Auditability, Data Transfers and Bottlenecks, Performance Unpredictability, Reputation Fate Sharing. This paper provides the information to evaluate and improve the existing and new cloud system by removing the Obstacles and Opportunities.

Assistant Professor, discusses IPSec an Edge over Security Protocol. Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset is vulnerability. Internet security relies upon a few classes of protocols, the most employed among those in the SSL/TLS family for web security for network layer security. Section 1 of the paper is about different types of security protocols. Section 4 shows how to secure sensitive information and it shows how maximum performance can be achieved in communication. Section 5 provides explanation about security in virtual network.

The authors say that Cloud computing is a method of sharing computer resources instead of using software or storage on a local computer. The key strengths of cloud computing are reliability, easy maintenance, measurable usage, resource sharing, device and location independence and no extra need of special hardware. The public cloud has an issue of Side Channel Attacks. This paper presents the study of security problems and thereby their solutions
to make the data more sheltered and thereby increase the usage cloud computing technology in India.

A group of faculty state that: Two of the most important problems in cryptography are concerned with the security. Most cryptographic mechanisms such as symmetric and asymmetric cryptography. However, all cryptographic techniques will be ineffective if the key distribution mechanism is weak. In quantum cryptography, quantum key distribution protocols (QKDPs) employ quantum mechanics to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key. By using Quantum Channel we can eliminate passive attacks like eavesdropping and therefore replay attacks.

Faculty claim that Honeypots are an exciting new technology with enormous potential for the security community. Honeypots fall under two main categories, Detection and Respond. Honeypots collect as much information as possible on the attack. The honeypot should operate in stealth mode so that the attacker would not know of its presence. Honeypots can be used for production purposes by preventing, detecting, or responding to attacks. Honeypots can also be used for research, gathering information on threats.

The author, presents a new highly automated approach for protecting Web applications against SQL injection that has both conceptual and practical advantages over most existing techniques. By using auditing to analyze the transactions to prevent malicious access and on the other hand Signature based approach is used to reduce the time taken to detect attacks. Moreover empirical evaluation is performed on wide range of web applications & WASP which automates the task very easily.

Professor claim that satisfactory results in terms of false positives and false negatives. The goal is to determine whether the two pages are suspiciously similar. She considered three page features that play a key role in making a phishing page look similar to a legitimate one. The proposed approach is inspired by open source anti-phishing solutions: the AntiPhish browser plug-in. Victims are typically convinced that they are visiting a legitimate page by judging the look-and-feel of a web site. Their approach was Signature Extraction and Signature verification.

A group of faculty in their article "Mitigating Online Fraud by Antiphishing Model With URL & Image based Webpage Matching". paper represents new anti phishing technique based on URL domain identity and image matching mechanism. It first identifies the related authorized URL. The image matching mechanism uses key point's detection and feature extraction methods. Two techniques i.e. URL domain identity and image webpage matching are combined, so this proposed work performs better than other existing tools.
38. Kumar Ch. V., Santhi G. (2012)
A couple of faculty claims to detect, near duplicates and duplicate spam mails in Cosdes (Collaborative Mail Detection System), fast by a new approach "SimHash". formed by users feedback, to block the subsequent near-duplicate spam's. This mitigates the effect of extremely common set members on data clusters. SimHash based approach is Fast, Flexible, Customizable (HtmlSimhash), Scalable and is patented: Uses an innovative tree structure, SpTrees, to store large amounts of e-mail.

Authors expresses their opinion that they believe, enterprise should analyse the companies / organization's security risks, threats, and available countermeasures before adopting Cloud technology. They have also point out some new emerging security problems Security, Standardization, Legal Aspects. The author suggests new directions: 1. Information-centric security (Data Loss Prevention vendors), 2. High Assurance Remote Server Attestation and 3. Privacy Enhanced Business Intelligence. Cloud fears largely stem from the perceived loss of control of sensitive data. The authors use trusted computing and applied cryptographic techniques to ensure security.

A pair of authors write in their article "Windows API based Malware Detection and Framework Analysis", propose the malware detection method based on extracting relevant application programming interface (API) calls from sub categories of malware. In this research project, the relevant APIs were extracted from each malware category and further refined using DCFS (Document Class-wise Frequency feature Selection) measure to classify the executable as malicious or benign. They focused on the Windows API calls, hence it will be limited to the detection of Windows PE malware.