Educational Administration: Theory and Practice
2024, 30(6), 4294-4322
ISSN: 2148-2403
https://kuey.net/
Research Article

Cyberguard: Cybercrime Risk Management And Insurance, Compensation, Punishment Model In The Digital Realm

Bandu B. Meshram[1*], Manish Kumar Singh[2]

[1*]Research Scholar, Nims, School Of Law, Nims University Rajasthan, Jaipur,(India).Email: bbmeshram.jes@gmail.com
[2]Head Of Law Department, Nims, School Of Law. Nims University Rajasthan, Jaipur,(India), Email:manishsinghlaw@gmail.com

Citation: Bandu B. Meshram, Manish Kumar Singh (2024), Cyberguard: Cybercrime Risk Management And Insurance, Compensation, Punishment Model In The Digital Realm, Educational Administration: Theory and Practice, 30(6), 4294-4322
Doi: 10.53555/kuey.v30i6.6695

ARTICLE INFO

ABSTRACT

: Cybercrime risks necessitate a comprehensive strategy to safeguard against evolving threats and potential impacts effectively. The researcher has proposed the research methodology to conduct research on cyber security risk, compensation and insurance to the victim of cyber-crime and punishment to the hacker. Researcher proposed The Cyber Risk Functional Model for cybercrime identification, projection, risk abatement, surveillance and governance strategy, formulating the design of data structure and algorithm for it and creating the instance for it using the data structure and proposed algorithms. This paper also explores the proposed Insurance Calculation Algorithms and Cyber Compensation Algorithm for cyber victims, compensating for the loss caused by cyber-attacks, and then proposes the algorithm for the calculation of punishment in terms of imprisonment and fines for cybercriminals for inclusion in cyber laws. In the digital realm, achieving algorithmic justice requires a delicate balance between mitigating risks, compensating cyber victims, and punishing cybercriminals. Cyber compensation algorithms have accurately assessed damages, including tangible and intangible losses, using data analytics and proposed algorithms for fair reimbursement. Similarly, algorithms for cyber insurance have considered breach severity and security measures to incentivize proactive cyber security. Proposed Punishment algorithms based on the gravity of the cyber crime will balance deterrence and rehabilitation, considering factors like intent and criminal history for fair sentencing. Transparency and accountability are crucial in algorithm development to ensure unbiased decisions. Harmonizing compensation and punishment can foster a digital ecosystem promoting fairness and trust. The proposed algorithms offers several benefits like comprehensive approach, tailored decision-making flexibility and adaptability, enhanced victim support and deterrent effect over statutory provisions alone. Lastly the researcher enumerates the various sections of IPC 1860, BNS2023, Cr.PC 1973 and ITA 2000 which foster the compensation, insurance and punishment for crimes with future research directions in the this research.

Index Terms – Cyber Risk assessment, Cybercrime Insurance, Compensation And Punishment, The Digital Realm.

1. Introduction

Cybercrime poses a multifaceted risk, demanding a comprehensive approach from risk identification through to management. In the realm of risk identification, understanding the evolving tactics of cyber criminals and vulnerabilities within systems is paramount[1]. This is followed by projecting potential impacts, encompassing financial losses, reputational damage, and legal repercussions. Refining these risks involves assessing their likelihood and severity, prioritizing them accordingly. Mitigation strategies must then be developed, integrating robust cyber security measures, employee training, and incident response protocols. Continuous monitoring ensures timely detection of threats, while an agile management plan allows for swift adaptation to emerging risks, ultimately safeguarding against the dynamic landscape of cybercrime.

Cyber insurance is a vital tool in today's digital landscape, offering protection against the rising tide of cyber threats. With attacks becoming more frequent and sophisticated, businesses face significant financial risks, ranging from data breaches to business interruptions and liability claims. Cyber insurance steps in to mitigate these risks by covering various expenses incurred in response to cyber incidents. Initially focusing on data breaches, cyber insurance has expanded its scope to include broader risks like business interruptions and social engineering fraud. However, the industry grapples with challenges such as accurately assessing and pricing cyber risk, addressing coverage gaps, and managing concerns about moral hazard. Despite these hurdles, the demand for cyber insurance continues to rise as businesses recognize the importance of protecting themselves against cyber threats. However, as demand increases, insurers may encounter capacity constraints and heightened competition, which can impact coverage availability and affordability, posing additional challenges for both insurers and insured parties alike. Thus, while cyber insurance provides a crucial safety net in the digital age, navigating its complexities requires a nuanced understanding of evolving cyber risks and insurance market dynamics.
Compensation for cyber-attacks is vital, countering financial losses and reputational harm businesses face. Cyber insurance provides dynamic financial safeguards, encompassing a spectrum of expenses associated with cyber-attack.. It typically includes costs for data breach response, cyber extortion, business interruption, and liability claims. Cyber compensation has evolved from focusing solely on data breaches to encompassing a broader range of risks like business interruptions and social engineering fraud. Yet, challenges persist in accurately assessing risk, addressing coverage gaps, and managing moral hazard concerns. With increasing demand for cyber compensation, insurers may face capacity constraints and heightened competition, affecting coverage availability and affordability.
Punishing cyber attackers [2] is essential to deter malicious behaviour and maintain order in cyberspace. It holds perpetrators accountable and discourages future crimes. Various forms of punishment, including criminal charges, civil penalties, and legal consequences, are prescribed by the legal system. Criminal charges may involve statutes like computer fraud and abuse laws, identity theft laws, and anti-hacking laws, leading to imprisonment, fines, probation, or victim restitution. Civil penalties may arise from lawsuits seeking damages for financial or reputational harm caused by cyber-attacks.
The legal system addresses cyber attackers through criminal charges, which may result in imprisonment, fines, probation, or restitution to victims. Civil penalties can also be imposed through lawsuits[1][2] seeking damages for financial or reputational harm. The evolution of cyber punishment has been influenced by the prevalence and severity of cybercrimes, prompting the enactment of laws specific to cybercrimes over time. The laws provide authorities with improved tools to prosecute offenders and impose appropriate penalties, reflecting advancements in technology and jurisprudence.

2. MATERIAL USED

This section discusses The literature survey used for the creation of proposed algorithms[8].

2.1 Cyber Risk Assessment

Cyber Risk assessment in information security is the process of recognizing, evaluating and ranking potential security risks.. Software risk can also be expressed Risk = { (Ri, Li, Xi) } Among them, Risk represents a software risk set. Ri represents software risks, Li represents the probability of occurrence of a risk, Xi represents risk results. Identify only(i) the software quality risk for cyber attack and(ii) Technology risk for cyber-attack (ii) the cybercrime attacks on software with respect to Risk and present in table forms for protected systems.
Inputs: (i) Assets (ii) Threat Sources (iii) Threat Events (iv) Vulnerabilities (v) Mitigating Controls (vi) Likelihood (vii) Adverse Impacts
In the context of cyber-attacks, risk can be defined as the measure of the potential threat posed to an entity's digital assets and operations. Cyber-attack risk is the product of the likelihood of a cyber-attack occurring and its potential impact on the targeted entity's digital systems and data.
Cyberattack_ Risk = Likelihood_of_cyberattack x Impact _of_cyberattack
Information security risks are the potential threats stemming from the compromise of confidentiality, integrity, or availability of information or information systems..
Likelihood: Probability [0, 1]. The likelihood probability can be categorized into : Category (High, Medium, Low) or Always, Often, Sometimes, Rarely, Never.you can represent software quality risk and technology risk for cyber-attacks in the format you provided:

Assessment of cyber Risk Impact: Risk exposure= P * I
where p is the probability of occurrence for a risk and I is the impact, impact is measured in terms of the cost to the software project due to cyber risk.
I = Cd * C * S

Where Cd = The cumulative count of custom-built components to be developed from scratch to avoid each cyber risk and C= Cost Of Each LOC to be developed. and S= The Average Component Size In LOC.

Note: Risk assessment is an art and not a science

2.2 Different Types of Risks

The tables outline the different types of risks, their likelihood (Li), and the resulting impact (Xi) with respect to cyber-attacks on software system. Below are the tables representing the software quality risk, technology risk for cyber-attacks, and the risk of cybercrime attacks on software systems with hypothetical values filled in for next-generation cybercrimes[1][2][8]:

(i) The cyber-attacks are enumerated in table 2.2

Table 2.2.1 Cybercrime Attacks on Software[12][18]

Ri (Technology Risk)	**Li (Likelihood- Low/Med)**	Xi (Impact on software systems)
Phishing Attacks	High	Identity Theft
Ransomware	High	Financial Loss
DDoS Attacks	High	Operational Disruption
Advanced Persistent Threats (APT)-	High	Long-Term Data Compromise
Cross-Site Scripting (XSS)	High	User Data Theft
OWASP top 10	High	OWASP Top 10 Attacks
Network Attack	High	DDOS, R2L, Probing

(ii) Cyber Attack due to Software Quality Risk is shown in Table 2.2.2

Table 2.2.2 Software Quality Risk for Cyber Attack[8][11]

Ri (Software Quality Risk)	**Li (Likelihood- Low/Med)**	**Xi (Cyber-attack risk impact)**
Inadequate Testing	Medium	Unauthorized Access
Poor Code Quality	Low	Data Breach
Outdated Software	Medium	System Downtime
Insufficient Security Protocols	Medium	Unauthorized System Access
Inadequate Error Handling	Low	System Exploits
Lack of Regular Updates	High	Proliferation of Zero-Day Attacks

(iii) The sample cases for Technological Risk for Cyber Attack are shown in table 2.2. 3[11]

Table 2.2.3 Technology Risk for Cyber Attack

Ri (Technology Risk)	**Li (Likelihood- Low/Med)**	**Xi (Cyber-attack risk impact)**
Legacy Systems	Medium	Service Disruption
Unpatched Vulnerabilities	High	Compromised Data Integrity
Weak Encryption	Low	Information Leakage
IoT Device Vulnerabilities	High	Network Infiltration
AI Exploitation	Medium	Automated Attacks
Cloud Storage Breaches	Medium	Large-Scale Data Exfiltration
Quantum Computing Attacks	Medium	Encryption Breakdown

(iv)The impact of next generation cyber crime with reason is shown in table in Table 2.2.4

Table 2.2.4 Next Generation cyber-crime[5]

Next Generation cyber crime	**Likelihood probability**	**Impact**	**Reason for impact**
AI-Powered Attacks	Very Likely	4 Severity: High	AI powered attacks can lead to widespread disruption and damage of protected critical infrastructure.
IoT Exploits	Likely	3-4 Severity: Moderate to high	depends on the number of compromised devices and the resulting harm.
Cryptojacking	Likely	1 Severity: Moderate	Cryptojacking can lead to significant financial losses for victims.
Deep fakes	Likely	1-3 Severity: Moderate to high	depends on the intent and impact of the deceptive content

Ransomware	Likely	3 Severity: High	Ransomware can cause substantial economic loss and functional impairment or operational disruption to organizations and individuals.
Quantum Computing Threats	Very Likely	4 Severity: Very high.	due to the potential to undermine critical encryption systems and compromise sensitive data.
Metacrime	Very likely-likely	1-2	Severity: Variable, depends on the characteristics and scale of the unlawful penal activities facilitated by emerging technologies.

These tables are designed to help organizations understand and prepare for potential risks associated with cyber-attacks by assessing the quality of their software, the technology they use, and the types of cybercrime they may face. The provided values should be customized to fit the unique context of the organization's systems and security measures.

2.3 Cost Involved Due To Data Breach.

Table 2.3.1 Array of potential financial losses[11]

Cost Type For Breach	**How cost Calculated using parameters**
Direct expenses/ Cost	Hardware replacement or direct monetary losses are categorized as direct expenses. For example, lost device replacement, ransomware, mo ney transfer fraud, or physical equipment destruction.
Investigation Cos t	Time spent investigating and remediating an incident. For exampl e, identifying how an adversary gained access to a webserver, rem oving malware from an infected machine, or resetting compromised credentials.
Business interruption	The interruption of operations or lack of service/resources availability. For example, employee downtime from laptop theft o r lost customers from unavailable websites, servers are not accessible.
Reputation Dama ge	Cost of decreased market share, loss of customers, or other reputa tion Impacts
Credit Monitorin g/Breach Notifica tion	Costs associated with notifying victims of a breach or credit monitoring costs.
Loss of Intellectu al Property	Costs stemming from theft of intellectual property ie Copy Right, Patent , other sensitive info

The Impact of cyber attack harm to : (i) Operations (ii) Digital Assets (iii) Individuals (iv) Other Organizations(v) the Nation

2.4 Rate Of Cyber Incidents

Data leakage, email scams, Device theft, Web site compromises, online platform issues, USB-related events, browsing mishaps constitute the primary categories of cyber security threats, encompassing scenarios where sensitive information is exposed, email-based intrusions occur, devices are compromised or lost, websites are attacked, and malware is spread through web browsing or USB devices. However, with the advent of technological advancements like AI algorithms, IoT, quantum computing, and similar innovations, the landscape of cyber threats is evolving towards next-generation crimes. These advancements open up new avenues for sophisticated attacks, including AI-powered breaches, IoT vulnerabilities, quantum computing-enabled encryption challenges, and other emerging threats. Additionally, miscellaneous incidents such as false alarms, misuse investigations, and DDoS attacks contribute to the multifaceted nature of cyber security challenges organizations face today[5].

2.5 Metrics to Measure Return On Attack

Measuring the return on attack[11] in cyber security involves evaluating the balance between the payoff gained by attackers and the costs incurred to execute the attack. The attacker profit is calculated by subtracting the cost to mount the attack from the payoff obtained. This metric provides a straightforward assessment of the financial gain achieved through malicious activities. Additionally, the return-on-attack metric, calculated as the payoff from the attack divided by the cost to mount it, offers a quantitative measure of the efficiency and effectiveness of an attack. By comparing the potential gains to the investment required, organizations can gauge the attractiveness of various attack vectors to malicious actors. These metrics aid in understanding the economics of cybercrime and can inform strategic decisions regarding resource allocation for defense and mitigation efforts.

Attacker profit = payoff from attack – cost to mount attack

Return-on-attack = payoff from attack / cost to mount attack

3. RESEARCH PROBLEM AND RESEARCH METHODOLOGY

This section presents Statement of Research Problem, and research methodology used in research.

3.1 Research Problem

The Research Challenge aims to investigate the efficacy and its applicability in addressing contemporary cyber offenses within the Indian context. The statement of research is titled as **Cyberguard: Cybercrime Risk Management And Insurance ,Compensation and Punishment Model In The Digital Realm**

This research aims to develop a comprehensive Cyber Risk Mitigation, Monitoring, and Management Model (CR4M) alongside a functional model and data structure design tailored to address evolving cyber threats. Leveraging this functional model, the study endeavors to devise algorithms that efficiently mitigate cyber risks, monitor digital environments for potential vulnerabilities, and manage cyber incidents effectively. Subsequently, the research extends its focus to propose innovative algorithms for calculating cyber insurance premiums and compensation, aiming to provide fair and accurate financial protection to individuals and organizations in the event of cybercrimes. Finally, the researcher discover algorithm to determine appropriate punishment measures for cybercriminals, seeking to establish a robust deterrent framework within the digital realm. This dynamic research initiative endeavors to offer a holistic approach to cyber risk management, integrating technological innovation with legal and financial frameworks to enhance cyber security resilience and foster a safer digital ecosystem for Insurance, Compensation and Punishment (ICP) Model in the digital realm.

Research Hypothesis: The implementation of the Cyberguard model significantly influences the management of cybercrime risk and the provision of compensation, insurance, and punishment measures within the digital realm.

3.2 Research Methodology Used

This section describes investigative approach with respect to types of research applied, cybercrime research design, population and sampling, data collection and measurement of the results [3]**.**

3.2.1Types of research applied

It is a doctrinal research known as pure theoretical research which involves systematic analysis of cybercrimes risks, its identification, projection, risk, monitoring, mitigation and management plan for combating cyber offences. As the research is critical, the research types applied is (i) exploratory study (ii) descriptive research (iii) experimental studies (iv) diagnostic study to do the qualitative research for in-depth understanding of the phenomenon of cybercrime risk assessment. A systematic review research design was conceptualized for this study.

3.2.2 Research Design

This work involves the handling of cyber-criminal cases and embarks on research in several stages. Research design is made with respect to

(i)Sample Design: It focuses on the sample design encompassing cybercrime offences and instances[6][7][18].

a) The normal network Traffic flow from source to destination and several categories of attacks that target network are Interruption(denial-of-service (DOS) attack), Interception: (e.g., wiretapping), Modification and Fabrication. The data set used for Attacks of KDD Cup 99 Data/NSL KDD Data set[6] have Probe, DoS, Remote to Local (R2L) U2R- User to Root attacks and partial instances are created[18][4].

b) There are several insecure web application maintained ie datasets available that researchers can use to study OWASP Top 10 attacks and their mitigations. Some of these datasets include: OWASP WebGoat, OWASP Juice Shop, Vulnerable Web Applications Repository (VWAR), Hackazon: an open-source ecommerce platform, Damn Vulnerable Web Application (DVWA), Security Shepherd.

c) Network Forensic Data Set[7] used for finding the attacks are**(i)**DARPA Intrusion Detection Data set (ii)KDD -CUP Intrusion Detection Data set (iii)NSL-KDD Intrusion Detection Data set and (iv)UNSW-NB1

d) Database cyber-attacks requires access to datasets that contain examples of real-world attacks, simulated attack scenarios, or vulnerabilities in database systems LIKE The Australian Defence Force Academy (ADFA) datasets, AWID (Agriculture, Water, and Environmental Cyber security Dataset}, CERT Insider Threat Data, Microsoft Research Malware Classification Challenge Dataset, NVD (National Vulnerability Database), Cyber security Datasets from CIC(network traffic) and . UNSW-NB15 Dataset, Cyber security Datasets from The Canadian Institute for Cyber security (CIC)

(ii)Observational Design: it explores observation of various real life case studies for the assessment of cyber risks.
Cybercrime Epidemic in India observed but not limited are [21][24][25]

a) Sextortion Surge: India Ranked Among Top 10 Source Countries for Sextortion Scams, Exploiting Victims via Phishing Emails.
b) Deceptive Withdrawals: Bangalore Police Investigate Fraudsters' Ability to Withdraw Large Sum Despite Blocked Debit Card.
c) App-Based Tragedy: Telangana Police Grapple with Suicides Linked to Loan App Blackmailing, Exposing Massive Money Lending Fraud.
d) WhatsApp Impersonation: Italian Surveillance Company Distributes Fake WhatsApp App to iOS Users, Targeting Individuals for Data Theft.
e) Recruitment Ruse: Indian Journalist Falls Victim to Elaborate Phishing Attack by Impersonating Recruiters from Prestigious University.
f) Fake Loan Apps: Mumbai Police Uncover Racket of Fraudulent Mobile Apps Masquerading as Prime Minister Loan Schemes, Swindling Thousands.
g) Bank Data Theft: Pune Police Bust Gang Stealing Bank Data, Suspect Involvement of Bank Employees in Selling Information to Cybercriminals.

(iii)Statistical Design: it also encompasses mathematical and statistical analyses of processes for the design of various algorithms used in this research.

(iv) Operational Design : Operational Design encompasses an entailing various processes involved into cybercrime risk assessment cases.

3.2.3 Material and Tool used.

(i)Literature (i)Legal Documents related to cyber laws (ii) textbooks for software analysis and design (iii)Journals specializing in law and technology (iv)Cyber security and technology-focused books. (v)Government Reports related to cyber offenses (vi) Google digging and sci-hub is also used for the literature survey.

(ii)Population and Sampling: In order to carry out the research, convenience sampling is used by considering the real life case studies on cybercrime .

(iii)Data Collection Procedure: In this research, two types of data i.e., primary data and secondary data is used. The observational design method is used to collect the primary data set.

3.2.4Measurement and Scaling

The ratio scale can be used to measure4 the precision and recall of the threat detection by investigator and the accuracy of judgment based on statistics[7].
(i)Precision = TruePositives(TP) / (TruePositives(TP) + FalsePositives(FP))
(ii)Recall = TruePositives(TP) / ((TruePositives(TP) + FalseNegatives(FN))
(iii)Accuracy = (TP+TN) / (TP+TN+FP+FN)
(iv)The traditional F measure is calculated as follows:
F-Measure = (2 * Precision * Recall) / (Precision + Recall)
Note :Maximizing precision will minimize the number false positives, whereas maximizing the recall will minimize the number of false negatives.
But as it is theoretical research, implementation of the model is not done.

4. PROPOSED CYBERCRIME RISK MITIGATION, MONITORING AND MANAGEMENT MODEL(CRM4)

Researcher establishes a thorough cyber-crime risk assessment plan[8][11] tailored to the software organization's needs involves several critical steps meticulously executed. Initially, the process commences with Cyber risk identification. Here, stakeholders, project managers, team members, and users collaboratively identify potential cybercrime risks spanning data breaches, malware attacks, phishing schemes, and insider threats. This collaborative effort yields a comprehensive understanding of the organization's threat landscape, categorizing risks accordingly. Following risk identification comes the imperative stage of risk projection. Identified risks undergo thorough analysis to determine their potential impact and probability of occurrence. This entails assessing the severity and likelihood of various threats materializing. Prioritizing risks based on severity constructs a risk table, offering a structured overview of the most critical cybercrime risks.
Subsequently, the risk refinement phase hones in on the most pertinent cybercrime risks. By refining risks above a predefined cutoff point and considering specific organizational conditions, resources can be focused on addressing the most significant threats effectively.

The final stage encompasses risk mitigation, monitoring, and management. Stakeholders, project managers, and team members collaborate to develop robust mitigation strategies and proactive risk management measures. This involves implementing technical controls like firewalls and encryption protocols, along with establishing policies to mitigate human-related risks such as social engineering , continuous surveillance, observation and management ensure the effectiveness of mitigation efforts, with regular updates to risk assessment documentation and tracking of risk status and maintaining a comprehensive risk information sheet serves as a central repository for essential risk details, facilitating informed decision-making and on-going risk management efforts.

External entities, including Users, Stakeholders, Project Managers, and Project Team Members, communicate with the Risk Management System. Stakeholders supervise the project, playing a crucial role in identifying risks and determining appropriate risk management steps. Project Managers oversee various project aspects and implement necessary mitigation measures, while Team Members provide valuable input on identified risks. Users contribute perspectives and insights aiding in risk identification. The process involves the Project Manager identifying Risk Categories, while stakeholders, users, and team members collectively identify associated risks. Team Members assess impact, probability, and mitigation strategies for each risk, with the system prioritizing risks based on probability and impact to determine Risk Exposure. Stakeholders and Project Managers collaborate on Risk Monitoring, Mitigation, and Management, ensuring regular updates on risk status. Lastly, the system continuously tracks and documents risks using formats such as the Risk Information Sheet.

The Proposed Cyber Crime Risk Mitigation, Monitoring And Management Model is known as CRM4

4.2 Systems Analysis For CRM4

This section proposes the systems analysis using ER Diagram and functional Model.

4.2.1 ER Diagram

The ER Diagram for database schema design[9] for cyber crime assessment process is shown in figure 1:

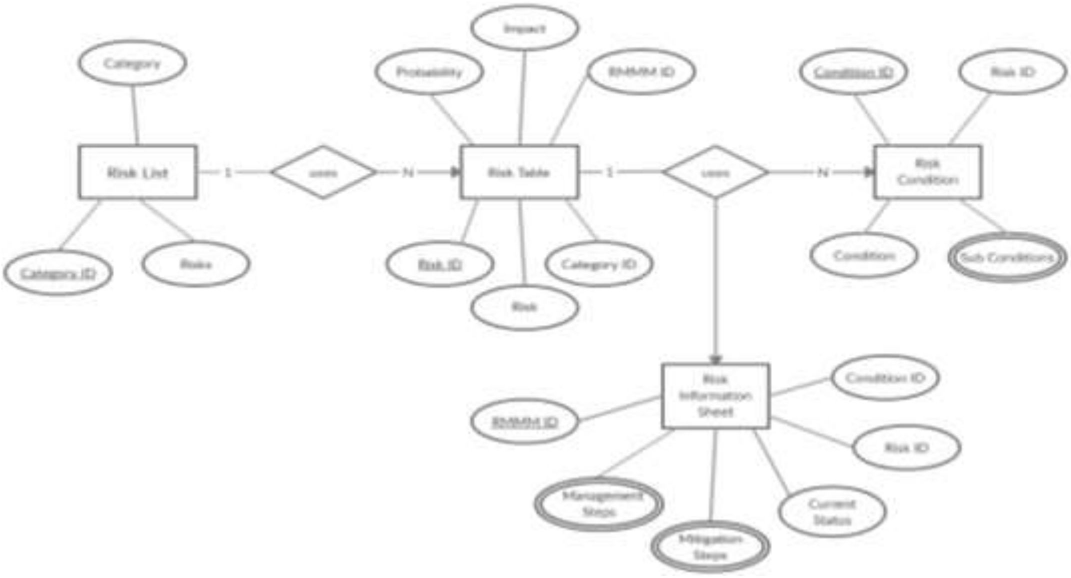

Figure 4.2.1 ER Diagram of Risk Management System

4.1.2 Functional Model

This section discusses the processes used in cyber risk management systems[8]

Context Diagram Functional Level 0:

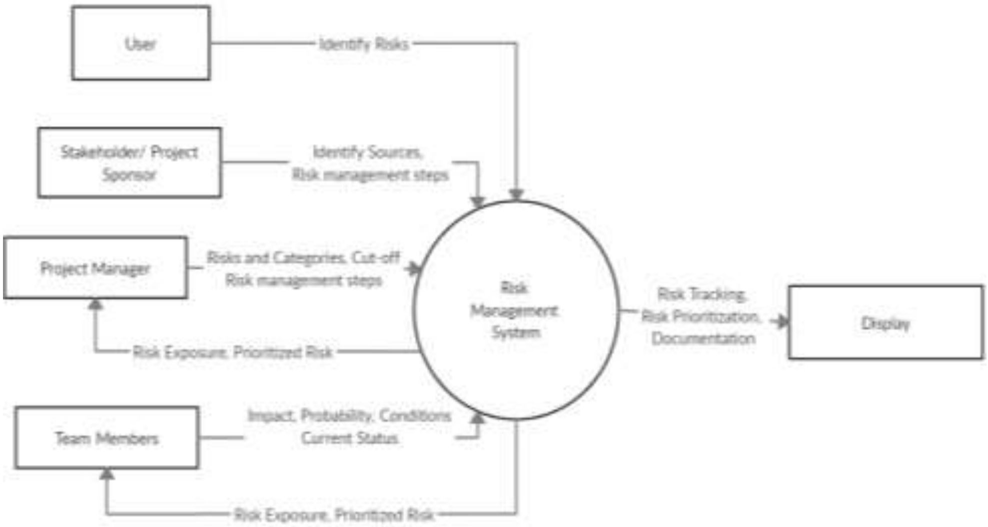

Figure. 4.1.2 Functional Level 0 of Risk Management System

4.1.3 Risk Management Information for the construction of CRM4 Model

From the statement of the research problem the researcher identified the processes, input to processes, output from each processes and data stored to read or write the data be processes. external entities as shown in Table 4.1.2

Table 4.1.2 :Risk Management Information for the construction of cyber crime **CRM4 ID Model**

Process	External Entity	Input	Output	Data Store
1. Risk Identification	1. Stakeholder, 2. Project Manager, 3. Team Members, 4. Users	1. Risk sources 2. Risk categories 3. Identified Risks	1. Update Risk List and Categories	Risk List
2. Risk Projection	1. Project Manager, 2. Team Members	1. Risk List and Categories 2. Impact, Probability 3. Cut-off	1. Prioritized Risks, 2. Risk Exposure	Risk Table
3. Risk Refinement	Team Members	1. Risk Table (top risks above cut-off) 2. Conditions	1. Update risk condition list	Risk Condition
4. Risk Mitigation, Monitoring, and Management	1. Stakeholder, 2. Project Manager, 3. Team Members,	1. Risk Table 2. Risk Condition 3. Mitigation Steps 4. Risk Management Steps 5. Current Status	1. Risk Tracking, 2. Documentation 3. Create Risk Information Sheet	Risk Informatio n Sheet

Functional Level 1:

The level 1 functional model has following processes:

1. Risk Identification: This process is used to specify threats to the project. Project Manager specifies the risk categories, then all the team members list risks (generic and product specific).
2. Risk Projection: In this process the team members then decide the impact, probability and cut-off of the risks. The system then sorts and prioritizes risks according to probability and impact and returns Risk Exposure. Only the risks above the cut-off are considered.
3. Risk Refinement: The team members discuss the conditions that lead to the occurrence of the risks. The sub-conditions are also stated.

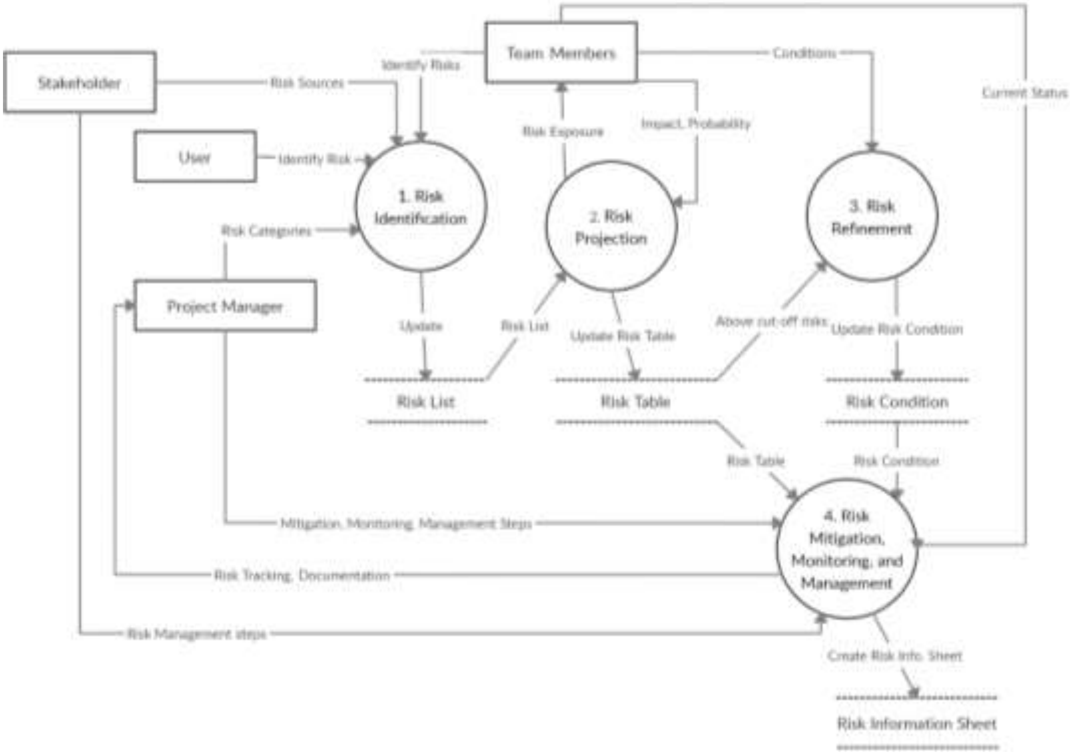

Figure 4.1.3 Level 1 functional Model of Risk Management System

4. Cyber Threat Risk Mitigation, Surveillance, and Governance Strategy:: The Stakeholder, Project Manager and Team Members decide on the Cyber Risk Mitigation, Monitoring and Management Steps. If the risk is avoidable then Risk Mitigation Steps are applied else Risk Management Steps are applied.
5. External Entities used in level 1 functional model are stakeholder ,project manager, team member and users.
6. The Data Stores are :Risk List: Risk Table: Risk Condition and Risk Information Sheet:

Functional Model Level 2

The level 2 Functional Model has following processes:

1. Risk Mitigation: The Project Manager identifies the avoidable risks and inputs risk mitigation steps.
2. Risk Monitoring: The Risk Mitigation steps, Risk Condition, Risk Table and Current Status of the risk are taken as input to tracks status of the risk.
3. Risk Management: For the unavoidable risks, the Stakeholders and Project Manager specify the Risk Management Steps.
4. Risk Information Sheet: This process combines all the details of the risks into one risk information Sheet per risk.
5. External Entities used are :Stakeholder: Project Manager, Team Members: 6.Data Stores used are Risk List, Risk Table, Risk Condition , Risk Management and Risk Mitigation and Risk Information Sheet:

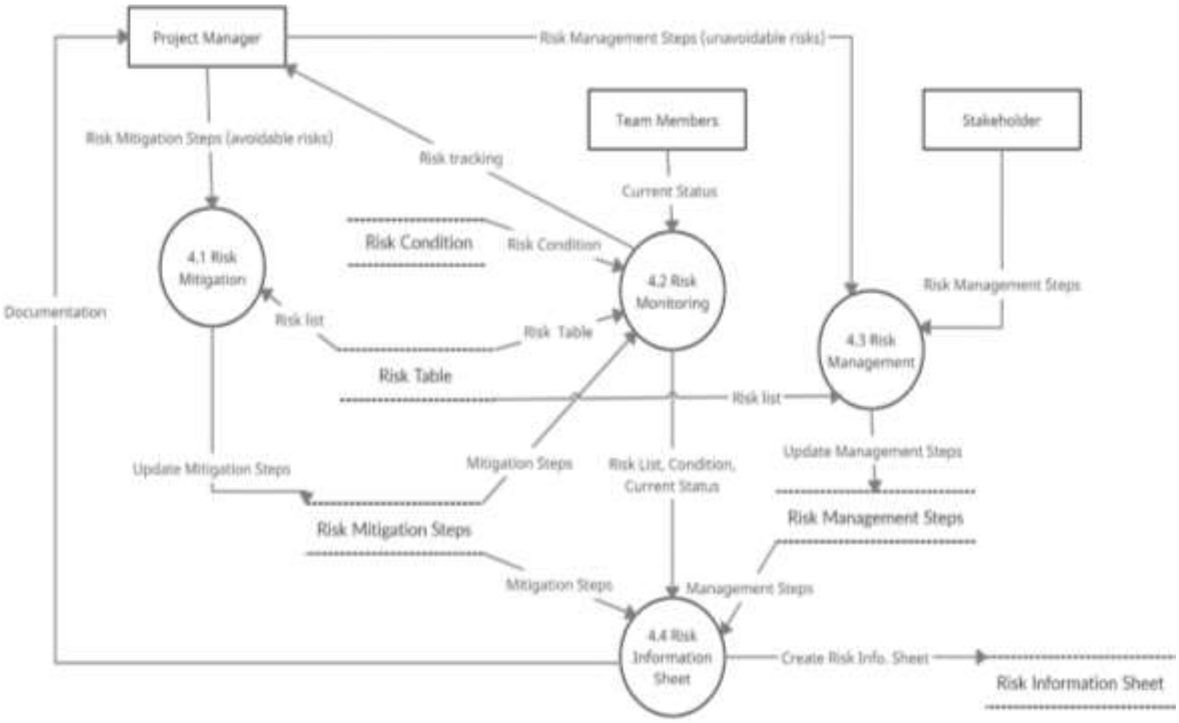

Figure. 4.1.3.1 Level 2 functional Model of Risk Mitigation, Monitoring and Management

4.2 System Design For CRM4

This section map the analysis of CR4M Systems to Design of CRM4

4.2.1 Data Structure Design

The ER Diagram is mapped with database schema design of the CRM4 Systems using ER to database mapping Rules[9].

1. Risk List: The identified risks both generic and cyber specific are specified with their categories.

Attributes: Category ID(varchar) Primary key, Category (varchar), Risks (Varchar)

2.Risk Table: It consists of risks, category, impact, probability, CRM4 pointer

Attributes: Risk ID(Alphanumeric) Primary key, Risk (Varchar), Category (Varchar) Foreign key, Probability (integer), Impact (integer), CRM4 ID(integer) Foreign key

3.Risk Condition: It has Risk condition and the sub-conditions that lead to occurrence of the risk

Attributes: Condition ID(integer) Primary key, Risk ID (Alphanumeric) Foreign Key, Condition (Varchar), Sub-Condition (varchar) (Multivalued Attribute)

4. Risk Information Sheet: It combines Risk Table, Risk Condition with Risk Mitigation and Management Steps.

Attributes: CRM 4ID (integer) Primary Key, Risk ID (Alphanumeric) Foreign key, Condition ID (integer) Foreign key, Management Steps (varchar) (Multivalued Attribute), Mitigation Steps (varchar) (Multivalued Attribute), Monitoring Steps (varchar) (Multivalued Attribute) Current Status (varchar), Owner (varchar), Date (Date time)

5. Risk Mitigation

Attributes: RiskID, MitigationID (Primary Key), Mitigation Steps (varchar)

6. Risk Management

Attributes: RiskID, ManagementID (Primary Key), Management Steps (varchar)

7. Risk Monitoring

Attributes: RiskID, MonitoringID (Primary Key), Monitoring step (varchar)

4.2.2 Algorithm Design: Cyber Crime Risk Assessment Plan

This section explore the algorithm design[10] for Cyber crime Risk Mitigation, Monitoring, and Management Model

The Cyber Crime Risk Assessment Plan[8] is structured into four key steps. Firstly, in the Cyber Risk Identification phase, potential cyber crime risks are identified through engagement with stakeholders, project managers, team members, and users. These cyber risks are then categorized and the risk list is updated accordingly. Following this, in the cyber Risk Projection step, the impact and probability of the identified risks are assessed. A cut-off point is established to rank cyber risks based on gravity/severity, and a risk table is constructed to delineate prioritized risks along with their exposure levels. Subsequently, in the Risk Refinement stage, the top cyber risks identified above the cut-off point undergo further refinement by considering specific conditions. The Cyber risk condition list is then updated to reflect any changes. Finally, in the fourth step, titled Risk Mitigation, Monitoring, and Management, strategies for mitigating identified risks[8] are proposed, and ongoing monitoring and management processes are put in place to address and respond to any emerging cyber threats

4.2.2.1 Algorithm 4.2.2.1. Cyber Risk Recognition

The algorithm named Risk detection aims to identify and categorize potential cyber risks faced by the software organization. It takes two input variables: the list of risk sources and the list of risk categories. The algorithm then iterates through each risk source and combines it with each risk category to form a new risk. These newly identified risks are stored in a list, resulting in an updated risk list and categories. Finally, the algorithm outputs this updated list of identified risks. This process ensures a systematic approach to risk identification, involving stakeholders, project managers, team members, and users to provide comprehensive input. The pseudo code for the "Risk Identification" algorithm outlines a process to identify and categorize potential risks faced by the software organization.

//* Listing of Algorithm 4.2.2.1.Risk Identification*//
Algorithm Name: Risk Identification
Input Variables:
riskSources (array or list)
riskCategories (array or list)
Output Variables:
updatedRiskListAndCategories (array or list)

Procedure : Risk Identification

```
1. Start
2. Function RiskIdentification(riskSources, riskCategories)
3.    Initialize an empty list: identifiedRisks
5.    // Iterate through each risk source
6.    For each riskSource in riskSources:
7.       // Iterate through each risk category
8.       For each riskCategory in riskCategories:
9.          // Combine risk source and risk category to form a new risk
10.          newRisk = riskSource + " – " + riskCategory
11.          // Add the new risk to the list of identified risks
12.          identifiedRisks.append(newRisk)
13.   Return identifiedRisks
14. End
```

4.2.2.2 Algorithm 4.2.2 2. Risk Projection

The algorithm named "Risk Projection" takes several input variables: the risk list and categories, impact, probability, and a cut-off value. First, the algorithm calculates the risk exposure for each risk by multiplying its impact by its probability. Then, it combines all the input variables into a matrix and sorts this matrix based on risk exposure in descending order. Next, the algorithm determines the number of risks to include in the prioritized list based on the cut-off value. It extracts the top risks from the sorted matrix and updates the risk table accordingly. Finally, the algorithm outputs the prioritized risks, their risk exposure, and the updated risk table, providing a structured overview of the most critical risks faced by the organization.

//*Listing of Algorithm 4.2.2 2: Risk Projection*//
Algorithm 4.2.2. 2. Risk Projection

Input Variables:
Risk List and Categories (array or list)
Impact (array or list)
Probability (array or list)
Cut-off (scalar)
Output Variables:
Prioritized Risks (array or list)
Risk Exposure (array or list)
Risk Table (array or list

```
1. Start
2. Function RiskProjection(riskListAndCategories, impact, probability, cutOff)
3.    Initialize empty arrays: prioritizedRisks, riskExposure
4.    Initialize an empty list: riskTable
.
```

```
5.    // Calculate risk exposure for each risk
6.    For each index i in range of length of riskListAndCategories:
7.       riskExposure[i] = impact[i] * probability[i]
8   // Combine risk list, categories, impact, probability, and risk exposure into a matrix
9.riskMatrix = Combine(riskListAndCategories, impact, probability, riskExposure)

10.   // Sort the matrix based on risk exposure in descending order
11.   SortDescending(riskMatrix, by="riskExposure")
12.   // Determine number of risks to include based on cut-off
13.   numRisksToInclude = Min(cutOff, Length(riskMatrix))
14.   // Extract top risks based on determined cut-off
15.   prioritizedRisks = ExtractTopRisks(riskMatrix, numRisksToInclude)

16.   // Update risk table with extracted risks
17.   For each index i in range of numRisksToInclude:
18.      riskTable[i] = prioritizedRisks[i]
19  Return prioritizedRisks, riskExposure, riskTable
20. End
```

4.2.2.3 Cyber.Risk Refinement Algorithm

The "Risk Refinement" algorithm iterates through each risk identified above the cut-off point and evaluates specific conditions provided as input. Within the algorithm, a loop is initiated to iterate through each risk in the risk table, while a nested loop is started to iterate through each specified condition. At each iteration, the algorithm checks if the current risk meets the condition and updates the risk condition list accordingly. Finally, the updated risk condition list is returned as the output of the algorithm.

Listing of Algorithm 4.2.2.3 Cyber Risk Refinement algorithm

Algorithm Name: Risk Refinement
Input Variables:
riskTable (array or list) - top risks above the cut-off
conditions (array or list)
Output Variables:
updatedRiskConditionList (array or list)
riskCondition (array or list)
Pseudocode:

```
1. Start
2. Function RiskRefinement(riskTable, conditions)
3.   Initialize an empty list: updatedRiskConditionList
4.   // Iterate through each risk in the risk table
5.   For each risk in riskTable:
6.      // Check if the risk meets any of the specified conditions
7.   For each condition in conditions:
8.         If risk meets condition:
9.            // Update the risk condition list with the condition
10.           updatedRiskConditionList.append(condition)
11.  Return updatedRiskConditionList
12.End
```

4.2.2.4 Algorithm . Cyber Risk Mitigation, Monitoring, and Management(RMMM)

To effectively mitigate risks, it is essential to develop comprehensive mitigation steps and risk management strategies tailored to identified vulnerabilities. Continuous monitoring and management of risks ensure proactive identification and response to emerging threats. Tracking the status of risks and documenting all activities related to risk assessment and management provide transparency and accountability throughout the process. Creating and maintaining a Risk Information Sheet enables the recording of essential details about each risk, facilitating informed decision-making and ensuring a structured approach to risk mitigation and management and Regularly review and update the risk minimization, oversight and control framework to adapt to evolving cyber threats and organizational changes

//*Listing of Algorithm 4.2.2.4: Vulnerability Reduction, Tracking and Organization Strategy Blueprint*//
Algorithm Name: RMMM
Input Variables:
riskTable (array or list)
riskCondition (array or list)
mitigationSteps (array or list)
riskMonitoringSteps (array or list)
riskManagementSteps (array or list)
currentStatus (array or list)
Output Variables:
riskTracking (array or list)
documentation (array or list)
riskInformationSheet (array or list)
Pseudocode
1. Start
2. Function RiskMitigationMonitoringManagement(riskTable, riskCondition, mitigationSteps, **riskMonitoringSteps** ,riskManagementSteps, currentStatus)
3. Initialize empty arrays/lists: riskTracking, documentation, riskInformationSheet
5. // Develop mitigation steps and risk management strategies for identified risks
6. For each risk in riskTable:
7. If risk exists in riskCondition:
8. Apply corresponding mitigation steps, riskMonitoringSteps and risk management strategies
10. // Continuously monitor and manage risks
11. While ongoingRiskMonitoring:
12. If any new risks identified or status changes:
13. Update currentStatus and riskTracking
14. // Document all activities related to risk assessment and management
15. Record all updates and changes in documentation
16. // Create and maintain a Risk Information Sheet
17. For each risk in riskTable:
18. Populate riskInformationSheet with essential details about each risk
19. Return riskTracking, documentation, riskInformationSheet
20. End

4.2.2.4 Applicability Of Algorithm On Real Life Case Study

Step 1 Cyber Risk identification [11][12][18[19][21][22][23][24][25]

Table 4.1 Risk dentification

The category of risk and risks are identified from the data set defined in section 3.2.2 Research Design (i)Sample Design.

Category ID	Category	Identified Risks
CAT001	Data Security	Data Breach, SQL Injection, Cross-Site Scripting (XSS)
CAT002	Network Security	(i)R2L (Remote-to-Local): unauthorized access from remote systems,(ii) L2R (Local-to-Remote): unauthorized access from local systems to remote systems to gain unauthorized access,(iii)Denial of Service attacks- ICMP flood, SYN flood, UDP flood, and HTTP flood attacks (iv) Probing :scanning and reconnaissance- port scanning, network mapping, and fingerprinting, ARP spoofing, DNS spoofing, or SSL/TLS interception.
CAT003	Endpoint Security	Securing endpoints (such as computer, laptops, mobile devices, and servers) from malware, ransom ware, unapproved access, and data breaches, Fileless Attacks, Zero-Day Exploits, Endpoint Exploitation, Insider threats(unauthorized data exfiltration, sabotage, or accidental data breaches).
CAT004	Application Security	OWASP Top Ten Attacks :(i)SQL Injection,(ii) Cross-Site Scripting (XSS), (iii)Broken Authentication,(iv)Sensitive Data Exposure, (v) XML External Entities(XXE),(vi)Broken Access Control, (vii) Security Misconfiguration,(viii) Insecure Deserialization,(ix) Using Components with Known Vulnerabilities, (x)Insufficient Logging and Monitoring

CAT005	Physical Security	(i)Unauthorized Access, (ii)Physical Intrusion ,(iii) Social Engineering, (iv)Lock picking and Bypassing Physical Locks ,(v)Tampering with Physical Security Systems ,(vi)Exploiting Weaknesses in Perimeter Defenses ,(vii) Insider Threats,(viii) Vandalism and Sabotage ,(ix) Physical Theft , (x)Terrorist Attacks.
CAT006	Social Engineering	(i)Phishing, (ii)Spear Phishing (iii) Whaling (iv) Pretexting: (v) Baiting: (vi)Tailgating (vii) Impersonation
CAT007	Email security	(i) Phishing (ii) Spear Phishing (iii)Whaling (iv) Business Email Compromise (BEC) (v)Malware Distribution (vi) Credential Theft (vii) Attachment-based Attacks.
CAT008	Operating systems window security	(i)Registry Attacks(exploiting the Windows Registry, execute malicious code at system startup, escalate privileges, hide malware, or disable security features, registry poisoning), (ii)Memory Attacks(buffer overflows, heap spraying, system crashes, unauthorized access, data exfiltration, or the execution of remote commands, execute arbitrary code, bypass privileges and security controls). (iii)Process Attacks,(malware injects code into legitimate processes ,data theft, privilege escalation, and persistence on compromised systems, manipulate their behaviour, compromise their integrity, or gain unauthorized access) (iv) Device Attacks (exploit vulnerabilities in hardware devices, drivers, or peripheral components, target devices such as network adapters, USB drives, printers, or storage devices to deliver malware, escalate privileges, or exfiltrate sensitive information, system compromise, data loss, or disruption of system functionality **(v)**Information Attacks (i)gather sensitive information from Windows systems, users, or applications(ii) teal sensitive data from compromised systems,(iii) identity theft, corporate espionage, financial fraud, or other forms of cybercrime.
CAT009	Browser Security	Browsers (i)XSS(ii)CSRF (iii)browser Hijacking (iv)Click jacking (v)Drive-by Downloads (vi) Phishing and Malicious Websites (vii) Man-in-the-Browser (MitB)

Step 2 Risk Projection
2.Algorithm Risk Projection output
The table 4.2 output of Algorithm 2. Risk Projection

Rank	Category	Risk	Impact	probability	Risk exposure
1	Application Security	Sensitive Data Exposure	3	3	9
2	Email Security	Business Email Compromise (BEC)	3	3	9
3	Email Security	Malware Distribution	3	3	9
4	Endpoint Security	Fileless Attacks	3	2	6
5	Endpoint Security	Zero-Day Exploits	3	2	6
6	Endpoint Security	Insider threats	2	2	4
7	Browser Security	XSS	2	3	6
8	Browser Security	CSRF	2	3	6
9	Browser Security	Phishing and Malicious Websites	2	3	6
10	Application Security	SQL Injection	3	2	6
11	- ---------	-------	-----	----	------

Step 3 **Refinement based on condition**
Algorithms: Refinement table output

To refine the risks based on the specified conditions (impact > 2 and probability > 2), we can implement the "Risk Refinement" algorithm and apply it to the provided data. the refinement table along is as below:

Table 4.3 Refinement of risk

Rank	Category	Risk	Impact	Probability	Risk Exposure
1	Application Security	Sensitive Data Exposure	3	3	9
2	Email Security	Business Email Compromise (BEC)	3	3	9
3	Email Security	Malware Distribution	3	3	9

Algorithm : Cyber RMMM Plan output

The risks based on the specified conditions (impact > 2 and probability > 2) and then apply the proposed algorithm to develop the mitigation steps, monitoring strategies, and management approaches, the output is Table 4.4:

Table 4.4 cyber RMMM Plan output

Risk	Mitigation Steps	Risk Monitoring Steps	Risk Management Steps
Sensitive Data Exposure	Encrypt sensitive data, implement access controls	Monitor data access logs, conduct regular data audits	Establish incident response plan, train employees on data security
Business Email Compromise (BEC)	Implement email authentication mechanisms	Monitor email traffic for anomalies, conduct phishing simulations	Implement multi-factor authentication, conduct employee awareness training
Malware Distribution	Install and regularly update antivirus software	Monitor network traffic for suspicious activity, conduct regular malware scans	Implement network segmentation, conduct employee cybersecurity training

4.3 Providing Security

For Table 4.1 Risk Identification, the researcher enumerate the security solutions as below[1][19][25]:

(i)Protecting against physical security threats requires implementing a layered approach to physical security, including measures such as access control systems, surveillance cameras, perimeter fencing, security guards, employee training, and emergency response plans. Regular security assessments and audits can help identify vulnerabilities and weaknesses in physical security measures, allowing organizations to implement appropriate countermeasures [25].

(ii)Protecting against social engineering attacks requires raising awareness among employees, implementing security policies and procedures, providing training and education on recognizing and responding to social engineering tactics, and implementing technical methods , such as email filtering, multifactor biometric authentication, and access controls, to mitigate the risk of exploitation.

(iii)Protecting Windows systems against the attacks requires implementing security measures, such as antivirus software, firewalls, intrusion protection systems, patch management, access controls mechanisms, monitoring and logging mechanisms and security awareness training for users.

(iv)Protecting against endpoint security threats requires a comprehensive approach having discretionary, role based, mandatory access control[9] ,network segmentation, and encryption[18], including the use of endpoint protection platforms (EPP), antivirus and antimalware software, intrusion detection and prevention systems (IDPS), load balancing, and regular security updates and patches

(v)Internet security examines the network attack, email-based attacks and, email-based attacks.

a) Each of the network attack[18] should Implement robust security measures, such as intrusion protection systems, firewalls, access controls, and regular security audits, can help organizations defend against these types of network attacks.
b) Protecting against email-based attacks[27] requires implementing robust security measures, such as email filtering, anti-spam solutions, antivirus software, email authentication protocols[27] (e.g., SPF, DKIM, and DMARC), and regular security assessments. Additionally, organizations should encourage employees to exercise caution when interacting with emails, especially those containing phishing links, attachments, or requests for sensitive information
c) Protecting against browser-based attacks[29] requires implementing security best practices, such as keeping browsers and plugins up-to-date, using reputable security software, enabling security features like sandboxing and click-to-play plugins, exercising caution when clicking on links or downloading files from unknown sources, and educating users about common attack techniques and how to recognize and avoid them.. In addition to proficient coding, web developers should prioritize secure coding practices and conduct regular vulnerability testing on their applications to minimize the risk of exploitation.

(vi) Data Base Security: For vulnerabilities in databases [9][28] the mitigation plan shall be to develop robust security measures such as biometric authentication, encryption of sensitive data, regular security audits, penetration testing , regularly monitor network traffic[18] for anomalies, conduct vulnerability scans and assessments, review access logs and audit trails, analyze security alerts, and conduct periodic security assessments and management plan .

(vii)Wholesome environment Security[11][18[19[: Regularly assess organization's strategies, processes, and structures to ensure they remain aligned with its goals and objectives (ii) stay flexible for adoption of advancements in technology[23], or internal developments . iii) be proactive to make adjustments to stay ahead of the curve, engage all employees at all levels in the review process to gather diverse perspectives and insights, fostering a culture of research collaboration (iv) aim for continuous improvement mind-set of continuous improvement, where feedback is valued, and lessons learned from both successes and failures are used to inform future decisions.

5.PROPOSED CYBER CRIME VICTIM'S INSURANCE AND COMPENSATION(IC) ALGORITHM

This section discover the algorithms for Cyber Crime Compensation and Insurance Coverage for Cybercrime attacks on the infrastructure. The compensation should be calculated on the basis of attacker profit and return on attack and cost involved due to data breach and the insured cost to the victim organization or business organization to the victim[13][14][15].

5.1 Cyber Crime Victim's Compensation Algorithm

Cybercrime compensation for victims necessitates a nuanced approach that considers various parameters to ensure fair redress. Firstly, the extent of financial loss incurred by the victim, including direct monetary theft, costs of recovery, and potential damages to reputation or business operations, forms a crucial aspect of compensation calculation. Additionally, the psychological impact, such as emotional distress and trauma, merits acknowledgment, as cyber-attacks can induce long-lasting psychological harm. Furthermore, the level of negligence or security lapses on the part of the entity responsible for safeguarding data must be assessed, influencing the degree of liability and compensation owed. Legal fees incurred during investigation and litigation, as well as any subsequent preventive measures to fortify cyber security, should also factor into the compensation package. Overall, a comprehensive evaluation that encompasses financial, emotional, and security dimensions is imperative for just cybercrime compensation.

In this algorithm, we calculate the compensation for cyber victims based on risk assessment, return on attack metrics, and the cost involved due to a data breach. The compensation is determined by considering the attacker's profit, return on attack, and deducting the cost incurred due to the data breach from it

Listing of Algorithm 5.1 Calculate Compensation

Function: CalculateCompensation(assets, threat_sources, threat_events, vulnerabilities, mitigating_controls, likelihood, adverse_impacts, attacker_profit, cost_to_mount_attack, cost_type_for_breach)

1. Initialize variables:
   assets: Information assets of the victim organization.
   threat_sources: Sources of potential threats to the organization's information assets.
   threat_events: Events that could lead to attack incidents or breaches.
   vulnerabilities: Weaknesses in the organization's information systems or processes.
   mitigating_controls: Controls implemented to mitigate risks and vulnerabilities.
   likelihood: Probability of occurrence of threat events.
   adverse_impacts: Adverse impacts of security incidents or breaches.
   attacker_profit: Payoff obtained by the attacker from the cyber attack.
   cost_to_mount_attack: Cost incurred by the attacker to mount the cyber attack.
   cost_type_for_breach: Array containing various types of costs involved due to a data breach.

2. Calculate Risk Assessment:
   Risk = Likelihood x Adverse_Impact
   Determine the risk associated with potential threat events by multiplying the likelihood with adverse impacts.

3. Calculate Return on Attack Metrics:
   Attacker_Profit = Payoff_from_attack - Cost_to_mount_attack
   Return_on_attack = Payoff_from_attack / Cost_to_mount_attack

4. Calculate Cost Involved Due To Data Breach:
Iterate through the cost_type_for_breach array:
Calculate the total cost involved due to data breach based on the parameters provided for each cost type (direct cost, investigation cost, Commercial downtime, Brand tarnishing, Credit surveillance
/breach notification, Intellectual asset depletion).

5. Determine Compensation:
Compensation = Attacker_Profit + Return_on_attack - Cost_Involved_Due_To_Data_Breach
[Compensation is calculated as the sum of attacker profit, return on attack, minus the cost involved due to data breach.]

6. Return Compensation.

End Function

In this algorithm, the researcher provide the algorithm to calculate the compensation for cyber victims based on risk assessment, return on attack metrics, and the cost involved due to a data breach is cal. The compensation is determined by considering the attacker's profit, return on attack, and deducting the cost incurred due to the data breach from it.

5.2 Cyber Crime Insurance Calculation Algorithm

Insurance coverage for cybercrime is becoming increasingly vital in today's digital landscape, offering financial protection and risk mitigation for businesses and individuals alike. Several key parameters influence insurance calculation for victims of cybercrime. Firstly, the nature and extent of the cyber-attack, including the type of breach (e.g., data theft, ransom ware), the scale of compromised information, and the duration of the incident, play a crucial role. Secondly, the specific coverage provisions within the insurance policy, such as coverage for data breach , legal expenses, Operational disruption cost, and extortion payments, need to be considered. Furthermore, the proactive approach taken by the insured entity towards cyber security, encompassing robust risk management strategies and strict adherence to regulatory standards, dynamically shapes insurance premiums and coverage limits, particularly in response to potential losses such as data breaches or system compromises.. Moreover, the industry sector and size of the insured organization are significant factors, as they determine the potential impact of a cyber-incident on operations and reputation. Overall, a comprehensive assessment of these parameters is essential for determining appropriate insurance coverage and premiums tailored to the unique cyber risk profile of each insured entity. The researcher proposed the Algorithm to Calculate Insurance Coverage For Cybercrime based on following mathematical formula
:
Total Insurance Premium = Base Premium + Additional Premiums – Discounts
Where :
Base Premium: Fundamental cost of insurance coverage.
Additional Premiums: Cost associated with specific risk factors and coverage enhancements.
Discounts: Reductions in the insurance premium offered by insurers.

Formation of Cybercrime Insurance Calculation algorithm

Algorithm 1: cybercrime insurance calculation algorithm discusses the building blocks at abstract level for cybercrime insurance calculation algorithm[13[14][15].

//*Listing of algorithms 5.2 Cybercrime Insurance Calculation
// This detailed explanation provides a comprehensive understanding of each step in the algorithm for cybercrime insurance calculation.
Algorithm 1: Cybercrime Insurance Calculation
Inputs:
financial_losses: {data_recovery_costs, business_interruption_expenses, extortion_payments, legal_fees, regulatory_fines}
insurance_coverage: {coverage_limits, deductibles, co-insurance_provisions}
risk_exposure: {probability_of_attack, severity_of_attack}
risk_appetite: Organization's willingness to accept risk
risk_management_practices: Measures to mitigate cyber risk
cyber_insurance_policy: Existing policy terms and conditions
Outputs:
premium: Calculated insurance premium
coverage_gap: Gap in insurance coverage

1. Initialization:
financial_losses: This array contains potential financial losses associated with next-generation cyber attacks. Examples include costs for data recovery, business interruption expenses, extortion payments, legal fees, and regulatory fines.
insurance_coverage: This array includes details of existing cyber insurance policies, such as coverage limits, deductibles, and co-insurance provisions.
2.Cyber Attack Risk Assessment
Conduct a comprehensive cyber risk evaluation estimate the organization's exposure to cyber-attacks. This involves analyzing the probability and severity of potential cyber threats.
3.Loss Calculation
Utilize actuarial analysis techniques to calculate the expected loss and probable maximum loss for different cyber-attack scenarios. This helps in understanding the potential financial impact of cyber incidents.
4.Evaluation of Existing Coverage
Assess the adequacy of existing insurance coverage in mitigating cyber risks. Compare the coverage provided by the current policies with the estimated financial losses and risk exposure.
5.Base Premium Calculation
Calculate the base premium using a formula that considers the organization's risk exposure, coverage requirements, and financial capacity. This forms the foundation of the insurance premium calculation.
6.Additional Premiums Calculation
Determine any additional premiums required to cover specific risk factors or enhance coverage beyond the base premium. This considers factors such as industry-specific risks and additional coverage enhancements.
7.Discounts Application
Apply discounts on the basis of organization's cyber risk management practices, cyber security maturity, and claims history. Effective risk management practices and a favourable claims history may result in reduced premiums.
8.Total Insurance Premium Calculation
Calculate the total insurance premium by summing up the base premium, additional premiums, and adjusting for any discounts. This provides the overall cost of insurance coverage considering various risk factors and discounts.
9.Gap Assessment in insurance coverage
Assess the gap in insurance coverage to identify the need for additional insurance or risk mitigation measures. This ensures that the organization's insurance coverage aligns with its risk exposure and financial capacity.
10.Policy Definition
Define the terms and conditions of the cyber insurance policy, including coverage scope, limits, deductibles, and co-insurance provisions. This ensures clarity regarding the coverage provided by the policy.
11.Continuous Monitoring
Continuously monitor changes in the cyber threat landscape and adjust insurance coverage and risk management strategies accordingly. This helps in staying proactive in mitigating emerging cyber risks.
12 Output:
Output the calculated insurance premium and coverage gap for next-generation cybercrime insurance. This provides valuable information for decision-making and risk management purposes.

5.3 Subroutine Algorithms Used In Cyber Crime Insurance Algorithm

The above cyber crime insurance algorithms is written in details.

5.3.1 Algorithm 3.3.1 Calculate Base Premium

Base Premium (BasePremium): The base premium is determined based on the organization's risk exposure, coverage requirements, and financial capacity which is based on the foolowing factors involved:

(i)Risk Exposure (risk_exposure): This includes the probability and severity of cyber-attacks. It could be represented as a combination of the likelihood of an attack occurring and the potential financial impact.
(ii)Coverage Requirements (coverage_requirements): This considers the desired scope of coverage, including the types of losses to be insured against and the limits of coverage.
(iii)Financial Capacity (financial_capacity): This refers to the organization's ability to bear the financial burden of potential losses that are not covered by insurance.

Listing for Algorithm 5.3.1 Calculate Base Premium

```
.//* The function combines these factors to calculate the base premium, considering the level of risk exposure, coverage requirements, and the organization's financial capability
Function: CalculateBasePremium(risk_exposure, coverage_requirements, financial_capacity)
1. Initialize variables:
  risk_exposure: The organization's risk exposure to cyber attacks, including probability and severity.
   coverage_requirements: The desired scope of coverage, including types of losses and coverage limits.
   financial_capacity: The organization's financial capacity to bear the burden of potential losses.
2. Calculate the base premium based on the provided inputs:
  BasePremium = BaseRate * AdjustedExposure * AdjustedCoverage
3. Determine the BaseRate:
   The BaseRate represents the baseline premium rate charged per unit of coverage.
  This could be determined based on industry standards, actuarial analysis, or insurer's pricing models.
4. Adjust for Risk Exposure (AdjustedExposure):
   AdjustedExposure = BaseExposure * RiskFactor
Where
   BaseExposure: Represents the baseline exposure level for the coverage requirements.
   RiskFactor: Represents the risk level based on the organization's risk exposure.
5. Adjust for Coverage Requirements (AdjustedCoverage):
  -AdjustedCoverage = BaseCoverage * CoverageFactor
Where
  BaseCoverage: Represents the baseline coverage amount required.
   CoverageFactor: Represents the adjustment factor based on coverage requirements.
6. Adjust for Financial Capacity:
   If financial_capacity is below a certain threshold:
    Apply a loading factor to reflect the increased risk to the insurer due to the limited financial capacity.
7. Return the calculated base premium.
End Function
```

5.3.2 Algorithm 5.3.2 Calculate Additional Premiums

Additional premiums may be necessary to cover specific risk factors or enhance coverage beyond the base premium. This calculation considers:

Risk Factors (risk_factors): These could include industry-specific risks, geographical location, or other factors that increase the likelihood or severity of cyber attacks.

Coverage Enhancements (coverage_enhancements): This refers to additional coverage options or enhancements beyond the basic policy, such as coverage for emerging cyber threats or regulatory compliance requirements.

In this algorithm, the additional premiums calculated for each risk factor and coverage enhancement are added to the total additional premiums (AdditionalPremiums) using the formula:

AdditionalPremiums=AdditionalPremiums+Calculated Additional Premium

//* Listing for algorithm 5.3.2 Calculate Additional Premiums*//

```
//* The function  evaluates the impact of these risk factors and coverage enhancements on the premium, determining any additional amount required.*//
Function: CalculateAdditionalPremiums(risk_factors, coverage_enhancements)
1. Initialize variables:
  risk_factors: Factors contributing to increased risk exposure, such as industry-specific risks.
   coverage_enhancements: Additional coverage options or enhancements beyond the basic policy.
  AdditionalPremiums = 0
2. Evaluate the impact of risk factors:
  For each risk factor in risk_factors:
    Calculate the additional premium associated with the risk factor:
      AdditionalPremiumRiskFactor = BaseRiskFactor * ImpactFactor
      Where:
        BaseRiskFactor: Represents the baseline additional premium for the risk factor.
        ImpactFactor: Represents the impact of the risk factor on the premium, determined based on actuarial analysis or insurer's risk assessment models.
```

```
      Add the calculated additional premium to AdditionalPremiums:
       AdditionalPremiums = AdditionalPremiums + AdditionalPremiumRiskFactor
3. Evaluate the impact of coverage enhancements:
   For each coverage enhancement in coverage_enhancements:
     -Calculate the additional premium associated with the coverage enhancement:
       AdditionalPremiumEnhancement = BaseEnhancement * EnhancementFactor
       Where:
          BaseEnhancement: Represents the baseline additional premium for the coverage enhancement.
  EnhancementFactor: Represents the impact of the coverage enhancement on the premium,
determined based on the specific coverage options selected or policy enhancements.
      Add the calculated additional premium to AdditionalPremiums:
       AdditionalPremiums = AdditionalPremiums + AdditionalPremiumEnhancement
4. Return the total additional premium (AdditionalPremiums).
End Function
```

This ensures that the total additional premiums reflect the cumulative impact of all risk factors and coverage enhancements on the insurance policy.

5.3.3Algorithm 5.3.3 Calculate Discounts on Insurance

Discounts can be applied based on the various parameters such as :
Risk Management Practices (risk_management_practices): These include measures taken by the organization to mitigate cyber risks, such as implementing robust cybersecurity protocols, incident response plans, and employee training.
Cybersecurity Maturity (cybersecurity_maturity): This reflects the organization's level of maturity in terms of cybersecurity practices and infrastructure.
Claims History (claims_history): This considers the organization's past history of insurance claims, including the frequency and severity of claims.
These three parameters scale is considered as 1:High, 2: Average, 3: Moderate(Poor)

```
//*Listing of Algorithms 5.3.3 . CalculateDiscounts algorithms *//
//* The function CalculateDiscounts evaluates these factors to determine any discounts
applicable to the premium, reflecting the organization's proactive risk management and
favorable claims experience.*//

Function:CalculateDiscounts(risk_management_practices, cybersecurity_maturity,
claims_history)
1. Initialize variables:
  risk_management_practices: Measures taken by the organization to mitigate cyber
risks.
   cybersecurity_maturity: Level of maturity in terms of cybersecurity practices and
infrastructure.
   claims_history: Organization's past history of insurance claims.
  Discounts = 0
2. Evaluate the impact of  cyber risk management practices:
   Determine the discount based on the effectiveness of risk management practices:
  //*   If  cyber risk management practices are highly effective:
     Apply a high discount rate.
    -If risk management practices are average:
      Apply a moderate discount rate.
     If risk management practices are poor:
     - Apply no discount or a minimal discount rate.*//)
(
     DiscountRiskManagement=BaseDiscountRiskManagement*
ImpactFactorRiskManagement
     Where:
     BaseDiscountRiskManagement: Represents the baseline discount for risk
management practices.
     - ImpactFactorRiskManagement: Represents the impact of  cyber risk management
practices on the discount rate.
3. Evaluate the impact of cyber security maturity:
//* Evaluate the impact of cyber security maturity:
  3.1 Determine the discount based on the organization's level of cybersecurity maturity:
    If cyber security maturity is high then  Apply a high discount rate.
     If cyber security maturity is moderate then   Apply a moderate discount rate.
```

- If cybersecurity maturity is low then Apply no discount or a minimal discount rate*//
Determine the discount based on the organization's level of cybersecurity maturity:
DiscountCybersecurityMaturity=BaseDiscountCybersecurityMaturity* ImpactFactorCybersecurityMaturity
Where:
BaseDiscountCybersecurityMaturity: Represents the baseline discount for cybersecurity maturity.
- ImpactFactorCybersecurityMaturity: Represents the impact of cybersecurity maturity on the discount rate.
4. Evaluate the impact of claims history:
//*Evaluate the impact of claims history:
Determine the discount based on the organization's past claims history:
If the claims history is favorable (few or no claims):
Then Apply a high discount rate.
If the claims history is moderate (some claims, but not excessive):
Then Apply a moderate discount rate.
If the claims history is unfavorable (frequent or significant claims):
Apply no discount or a minimal discount rate.*//
Determine the discount based on the organization's past claims history:
DiscountClaimsHistory = BaseDiscountClaimsHistory * ImpactFactorClaimsHistory
Where:
BaseDiscountClaimsHistory: Represents the baseline discount for claims history.
ImpactFactorClaimsHistory: Represents the impact of claims history on the discount rate.
5. Combine the discounts from risk management practices, cybersecurity maturity, and claims history:
Discounts = DiscountRiskManagement + DiscountCybersecurityMaturity + DiscountClaimsHistory
6. Return the total discounts (Discounts).
End Function

These formulae provide a structured approach to calculating the base premium, additional premiums, and discounts, considering various risk factors, coverage requirements, and organizational characteristics.

5.4 Insurance Coverage Gap Calculation Algorithm

Insurance coverage gap calculation algorithm[16][17] is called by Insurance Calculation Algorithm is illustrated in listing Listing of Algorithms 5.4 . Insurance Coverage Gap algorithms .

//*Listing of Algorithms 5.4 . Insurance Coverage Gap algorithms *//
//*Main Subroutine: Insurance coverage gap calculation algorithm Under Insurance Calculation Algorithm *//
Algorithm 5.4 Name : **Insurance Coverage Gap algorithms.**
Function: AssessCoverageGap(financial_losses, insurance_coverage, Insurance_Premium)
1. Initialize variables:
financial_losses: Array containing potential financial losses associated with next-generation cyber attacks.
insurance_coverage: Array including details of existing cyber insurance policies (coverage limits, deductibles, co-insurance provisions).
Insurance_Premium: Total insurance premium calculated for next-generation cybercrime insurance.

2. Calculate Total Financial Losses:
Total_Financial_Losses = Sum of all elements in financial_losses array.

3. Calculate Total Coverage Provided by Existing Policies:
Total_Coverage_Provided = Sum of coverage limits in insurance_coverage array.

4. Calculate Deductibles and Co-insurance:
Total_Deductibles = Sum of deductibles in insurance_coverage array.
Total_Co-insurance = Sum of co-insurance provisions in insurance_coverage array.

5. Calculate Net Coverage Provided by Existing Policies:
Net_Coverage_Provided = Total_Coverage_Provided - Total_Deductibles - Total_Co-

```
insurance
   [Net coverage provided after deductibles and co-insurance]

6. Determine Coverage Gap:
  Coverage_Gap = Total_Financial_Losses - Net_Coverage_Provided

7. Return Coverage_Gap.

End Function
```

5.5 Jeman Insurance (JI) CalculationAlgorithm

This is the dynamic algorithm for deciding the insurance cover for the victim

//*Listing of Algorithm 5.5 for: Cybercrime Insurance Calculation *//

Algorithm 5.5 Name : Cybercrime Insurance Calculation

Variables:
- financial_losses: Array of potential financial losses
- insurance_coverage: Array of insurance coverage options
- risk_exposure: Estimated risk exposure for next-generation cyber attacks
- premium: Calculated insurance premium
- coverage_gap: Gap in insurance coverage

Inputs:
- financial_losses: {data_recovery_costs, business_interruption_expenses, extortion_payments, legal_fees, regulatory_fines}
insurance_coverage: {coverage_limits, deductibles, co-insurance_provisions}
risk_exposure: {probability_of_attack, severity_of_attack}
risk_appetite: Organization's willingness to accept risk
risk_management_practices: Measures to mitigate cyber risk
cyber_insurance_policy: Existing policy terms and conditions

Outputs:
premium: Calculated insurance premium
coverage_gap: Gap in insurance coverage

Procedure:
1. Initialize{ financial_losses array} with {potential financial losses} associated with cyber attacks.
2. Initialize{ insurance_coverage array} with details of existing cyber insurance policies.
3. Conduct a risk assessment to estimate the{ organization's risk exposure} to cyber-attacks.
4. Calculate the {expected loss and probable maximum loss} for different cyber attack scenarios using actuarial analysis techniques.
5. Evaluate the adequacy of existing insurance coverage to{ mitigate cyber risks.}// Risk Management strategy is in 3.2.2 Algorithm Design: Cyber Crime Risk Assessment Plan

6. Determine the {insurance premium }based on the estimated risk exposure, coverage requirements, and financial capacity.
Call insurance premium algorithm()
7. Assess the {gap in insurance coverage} call {gap in insurance coverage} //*3.4 Insurance Coverage Gap Calculation Algorithm*//
AND
identify the need for{ additional insurance or risk mitigation measures cost}.// .}//* Risk Management strategy is in 3.2.2 Algorithm Design: Cyber Crime Risk Assessment Plan*//

8. Define the terms and conditions of the cyber insurance policy, including coverage scope, limits, deductibles, and co-insurance provisions.
9. Continuously{ monitor changes in the cyber threat landscape} and adjust{ insurance coverage and risk management strategies} accordingly.
10. Output the {calculated insurance premium }and {coverage gap }for cybercrime insurance.
Call calculated insurance premium, algorithm //* 3.3.1 Algorithm 3.3.1 Calculate Base Premium*//

call coverage gap for cybercrime insurance. } //*3.4 Insurance Coverage Gap Calculation Algorithm*//

End Algorithm

6. PROPOSED CYBERCRIME PUNISHMENT(P) CALCULATION ALGORITHMS

The researcher not only identified the range of possible punishments for cybercrimes, including fines, imprisonment, community service, or rehabilitation programs but also classified the severity or gravity of punishment corresponding to each cyber risk category. For instance, low-risk cyber crimes were deemed to warrant lighter punishments, whereas extreme-risk cybercrimes were determined to necessitate harsher penalties. Additionally, consideration was given to factors such as the nature of the crime, the intent of the perpetrator, the extent of harm caused, and any aggravating or mitigating circumstances. Principles of proportionality and consistency were utilized in assigning punishments, ensuring that similar cybercrimes received comparable penalties.

By following this algorithmic approach, justice systems can effectively calculate punishments for cybercrimes based on their likelihood probability and impact, thereby deterring future offenses and promoting cyber security awareness and compliance.The mathematical formula for Threat Assessment involves assessing the likelihood probability and impact of potential cyber threats. While likelihood probability and impact are typically qualitative assessments, they can be converted into numerical values for computational purposes. However, the assessment itself is often based on expert judgment,evidence, historical data, threat intelligence, and risk analysis methodologies rather than a straightforward mathematical formule.

6.1 Cyber Threat Assessments

The formulation for threat assessment is illustrated below[[8][11].

(i) Nevertheless, we can represent the process of Threat Assessment mathematically as follows:

1. Likelihood Probability (L)
- Represented as a numerical value based on expert assessment or statistical analysis.
- It can be denoted as , where ii represents the category of likelihood (e.g., Very Likely, Likely, Unlikely).
- Example: If likelihood is assessed on a scale of 1 to 3 (with 3 being Very Likely and 1 being Unlikely), Li could be assigned values such as 3, 2, and 1 for Very Likely, Likely, and Unlikely categories, respectively.

2. Impact (I)
- Also represented as a numerical value based on expert judgment or analysis.
- Denoted as , where j represents the category of impact (e.g., Minor, Moderate, Major).
- Example: Similarly, if impact is assessed on a scale of 1 to 3 (with 3 being Major and 1 being Minor), Ij could be assigned values like 1, 2, and 3 for Minor, Moderate, and Major categories, respectively.

Once likelihood probability and impact are quantified, they can be multiplied to calculate the Risk Score:

$Risk=\sum i\sum jLi\times Ij$

This formula represents the aggregation of likelihood and impact assessments across all categories to derive an overall risk score. However, the specific method for assigning numerical values to likelihood and impact, as well as the calculation of the risk score, may vary depending on the risk assessment framework and methodology employed by an organization or jurisdiction.

(ii)The formula for Risk Assessment involves calculating the overall risk score by multiplying the numerical values assigned to the likelihood and impact categories. Here's the formula:

Risk=∑i=1n∑j=1m (Li×Ij)

Ie i=1 to n and j=1 to m

Where: represents the numerical score assigned to likelihood category i ;Ij represents the numerical score assigned to impact category j, n is the total number of likelihood categories and m is the total number of impact categories.

This formula calculates the risk score by summing the products of the numerical scores of likelihood and impact categories across all possible combinations.

(iii). Assign Numeric Values: To convert the qualitative likelihood and impact classifications into numeric values, we assign numerical scores to each category based on expert judgment, historical data, or risk analysis methodologies.

- **Assigning Numeric Values to Likelihood (L):** Likelihood categories (e.g., Very Likely, Likely, Unlikely) are assigned numerical scores based on their perceived probability or frequency of occurrence.
- Let Li represent the numerical score assigned to likelihood category ii, where i ranges from 1 to n (number of likelihood categories). The assignment of numerical values can be done based on a scale where higher values indicate higher likelihood. For example, if there are three likelihood categories(i)$L1$ for Unlikely = 1 (ii)$L2$ for Likely = 2 (iii)$L3$ for Very Likely = 3

- **Assigning Numeric Values to Impact (I):** Impact categories (e.g., Minor, Moderate, Major) are similarly assigned numerical scores based on the perceived severity or consequence of the impact.
- Let Ij represent the numerical score assigned to impact category j, where j ranges from 1 to m (number of impact categories).

. For example, if there are three impact categories(i)$I1$ for Minor = 1 (ii) $I2$ for Moderate = 2 (iii) $I3$ for Major = 3(higher impact)

With these assignments, the risk assessment formula calculates the overall risk score by summing the products of the numerical values assigned to likelihood and impact categories.

(iv). Calculating The Risk Score function: The formula for calculating the risk score for each potential cyber threat involves multiplying the numerical values assigned to the likelihood and impact categories.is
Risk Score=Likelihood Value×Impact ValueRisk Score
This calculation helps prioritize and assess cyber threats based on their potential risk levels, allowing organizations to allocate resources effectively for mitigation and response efforts..

(v)Formulation for Threshold Calculation

To establish thresholds for risk categories based on the calculated risk scores, organizations often define categories that represent different levels of risk. These categories help in prioritizing and managing cyber threats effectively. The common approach to defining cybercrime risk categories along with a formulation for threshold calculation:
(i)Low Risk**:** Minor cyber threats with minimal low probability and impact may not pose substantial risk to organizational assets or operations..(ii)Medium Risk: Moderate cyber threats may disrupt operations or cause minor damage to assets..(iii)High Risk**:** Highly likely cyber threats with significant impact demand immediate attention for organizations asset, operational, or reputational protection. Thresholds for risk categories can be established based on the range of risk scores calculated using the risk assessment formula. Define the range of risk scores that correspond to each risk category based on organizational risk tolerance, industry standards, and best practices.
For example, consider the following ranges for risk categories (i)Low Risk: Risk Score <= X1 (ii) Medium Risk: X1 < Risk Score <= X2 (iii)High Risk: Risk Score > X2
Threshold values (X1 and X2) are determined based on risk appetite, historical data, and regulations. Periodic review and adjustment ensure alignment with organizational risk tolerance and changing priorities, maintaining effectiveness over time.By establishing clear thresholds for risk categories, organizations can effectively prioritize cyber threats, allocate resources, and implement appropriate controls to mitigate risks and protect critical assets and operations.

6.2 Algorithm Cyber Threat Risk Assessment and Punishment

By analysing the various functionalities and formulation, the proposed Cyber Threat Risk Assessment and Punishment –imprisonment and fine Calculation (CTRAPC) Algorithm is given as below:

//*Listing for algorithm 6 Cyber Threat Risk Assessment and Punishment – imprisonment and fine Calculation (CTRAPC) Algorithm *//

Algorithm 6 Name: Cyber Threat Risk Assessment and Punishment – imprisonment and fine Calculation (CTRAPC) Algorithm
Input Variables
Likelihood of Cyber Threat (L): Categorical variable (Very Likely = 4, Likely = 3, Unlikely = 1)
Impact of Cyber Threat (I): Categorical variable (Minor = 1, Moderate = 2, Major = 4)
Output Variables
Maximum Punishment:
Maximum Imprisonment Duration (MI)
Maximum Fine Amount (MF)
Mathematical Formulas:
Risk Calculation:
Risk=L×I
Punishment Calculation:
a. For Imprisonment (PI):
PI=α×Risk+b
Where
α
α is a coefficient representing the rate of increase in imprisonment duration per unit

increase in risk, and 'b' is a constant representing the base duration of imprisonment.

b. For Fine (PF):
PF=β×Risk+c
Where
β
β is a coefficient representing the rate of increase in fine amount per unit increase in risk, and 'c' is a constant representing the base fine amount.

Algorithm

1. Threat Assessment
Assess the likelihood probability and impact of potential cyber threats.
2.Assign Numeric Values
Convert the qualitative likelihood and impact classifications into numeric values.
3.Calculate Risk Score
Calculate the risk score for each potential cyber threat by multiplying the likelihood and impact values.
4.Punishment Calculation
Determine the maximum punishment for each risk category.

4.1For Imprisonment

Calculate the maximum imprisonment duration (MI) based on the risk score using the formula
MI=PI×Risk+b

4.1 For Fine

Calculate the maximum fine amount (MF) based on the risk score using the formula:
MF=PF×Risk+c
4 Thresholds and Categories
Establish thresholds for risk categories based on the calculated risk scores.
5 Assign Punishments
Based on the risk category, assign appropriate maximum imprisonment duration (MI) and maximum fine amount (MF) using the calculated formulas..

This Cyber Threat Risk Assessment and Punishment Calculation (CTRAPC) algorithm incorporates precise mathematical formulations for calculating the maximum imprisonment duration and fine amount based on the assessed risk score, ensuring consistency and fairness in sentencing for next-generation cyber threats.

7.INDIA'S SATUTE JURISPRUDENCE FOR INSURANCE COMPENSATION AND PUNISHMENT

This section discusses the statute legislation for insurance, compensation and punishment

7.1 Compensation

The compensation and punishment scheme is provided by CrPC and Bharatiy Nagrik Suraksha Sanhita (BNSS)2023, and IT Act based on the statute legislation, expert opinion and judgment based on the gravity of the cybercrime.

Table 7 Compensation by CrPC , BNSS, IT Act ,

Compensation by CrPC[30] **, BNSS**[34]**, IT Act**[31] **,**					
CrPC CrPC 1973- Chapter Xxvii The Judgement		BNSS 2023 BNSS Chapter XXIX The Judgement		IT Act 2000/2008 Chapter IX Penalties, Compensation And Adjudication	
Section	Purpose	Section	Purpose	Section	Purpose
357	Directive for restitution	395	Order To pay compensation	43	Sanction and restitution for harm to computer systems, hardware, etc..
357A	Restorative Justice Program	396	Victim Compensation scheme	43A	Compensation for failure to protect data
357B	Compensation shall be supplementary to the penalty prescribed under Section 326-A or Section 376-D of	396	Victim Compensation scheme	44.	Penalty for non-disclosure of information, submission of returns, etc

	the IPC.				
357-C	Treatment of victim	397	Treatment of victim	45	Residuary penalty
358	Restitution to individuals wrongfully detained	399	Compensation to persons groundlessly arrested		

7.2 Insurance Provided by ITA 2000

Specific sections of the Information Technology Act (ITA) of India[31] that may touch upon aspects of cyber insurance and risk management in the context of digital transactions and data protection include: (i)Section 43 and 43A:. It mandates that a body corporate (including companies) possessing, dealing, or handling any sensitive personal data or information in a computer resource, which it owns, controls or operates, is liable to pay damages to the person affected by any wrongful loss or gain due to the negligence in implementing and maintaining reasonable security practices and procedures.(ii)Section 70B:. While not directly related to insurance, it underscores the importance of protecting critical information infrastructure, which may indirectly influence risk management strategies, including the consideration of cyber insurance.(iii) Section 79 of the ITA deals with the liability of intermediaries for hosting or publishing content online, it indirectly facilitates the provision of cyber insurance. These sections, along with others in the ITA and related regulations, contribute to the broader legal framework governing cyber security and data protection in India, which in turn may inform and shape considerations for cyber insurance and risk management practices.

7.3 Punishment for cyber crimes

In India, the punishment for cybercrimes is determined by both the Indian Penal Code (IPC), Bharatiy Nyaya Sanhita(BNS),2023 and the Information Technology Act (ITA). According to IPC 1860 Chapter III OF PUNISHMENTS (sec53 to sec75) and BNS Chapter II OF PUNISHMENTS (sec 4 to 13) , section 53 IPC and sec 4 BNS states that , the severity of punishment varies depending on the nature and gravity of the offenses to which offenders are liable for Death, imprisonment of life, simple or rigorous imprisonment with the hard work , forfeiture of property and fine respectively.

Table 7.3 **Punishment under IPC and BNS**

Punishment under IPC[33] and BNS [32]			
IPC		**BNS**	
Section	Purpose	Section	Purpose
53	Punishments	4	Punishments
54,55,	Commutation of sentence of death, imprisonment for life	5	Commutation of sentence
60	In some cases, prison sentences can be tough or light.	7	In certain cases of imprisonment, prison sentence can wholly or partly rigorous or simple
63	Amount of fine	8(1)	Amount of fine, liability in default of payment of fine, etc.
71	Limit of punishment of offence made up of several offences	9	Limit of punishment of offence made up of several offences
72	many paths of offences, uncertain destination for judgement	10	Punishment of person guilty of one of several offences, the judgment stating that it is doubtful of which
73	Isolation confinement	11	Solitary confinement
75	Enhanced punishment for certain offences under Chapter XII or Chapter XVII after previous conviction	13	Enhanced punishment for certain offences after previous conviction

The IT Act has array of sections for punishment and offences described in chapter XI OFFENCES. Various sections for digital communication or transmitting electronic material to do cyber offences such as 65 (Tampering computer documents), 66. (Computer offences), 66A(sending offensive communication), 66B(dishonestly receiving stolen computer assets), 66C (identity fraud), 66D (cheating by personation), 66E(violation of privacy), 66F(cyber terrorism). 67. (Digital obscene material), 67A(sexually explicit act), 67B (depicting children in sexually explicit act), 67C(role of intermediaries), 72. (Violation of confidentiality and privacy), 72A. (Breaching a legally binding agreement / contract), 73(Falsifying electronic signature certificates), 74(Publication for fraudulent purpose) and the like are included in ITA.

The judiciary plays a crucial role in deciding the punishment for cyber criminals, taking into account factors such as the type of cybercrime committed, its impact on individuals or society, the intent behind the crime, and the criminal history of the offender. The punishments can range from fines to imprisonment, with the judiciary striving to ensure that the punishment fits the crime while also serving as a deterrent against future cyber offenses.

8. IMPLICATIONS AND PROSPECTS FOR FURTHER STUDY

This section discusses the summary of the work, its advantages over written statutes and future research direction for implementing the decision making tools for **CRM4 and C(JI)P Model.**

8.1 Conclusion

The proposed algorithms combines the notion of safeguarding against cyber threats with risk management strategies(CRM4**)**, comprehensive compensation, insurance for cyber victims, and punishment(C(JI)P Model) for cyber hackers. The researcher has also created the instance of CRM4 and explores security measures for different arrays of cybercrimes**.** The cyber risk impact may involve providing immediate compensation to victims for urgent needs while leveraging cyber insurance to cover broader financial losses and recovery efforts. Cybercrime Jeman Insurance (JI) Algorithm is designed to decide the financial impact of cyber incidents on businesses and individuals. It typically covers insurance cost , cost of legal fees, investigation costs, and even compensation to victims. The cyber insurance provides essential financial protection against evolving cyber risks, but businesses must carefully assess their needs and work with insurers to ensure appropriate coverage. The cyber compensation(C) provides essential financial protection against evolving cyber risks, but the industry must navigate challenges to ensure adequate coverage for businesses facing cyber threats. The punishment (P) for cyber attackers is crucial for maintaining the integrity and security of cyberspace. While legal systems have made strides in addressing cybercrimes, challenges remain in effectively prosecuting offenders and enforcing penalties, particularly in cases involving complex jurisdictional and attribution issues. Continuously refine the punishment algorithm based on feedback, emerging threats, and changes in the cybercrime landscape, regularly updating risk assessments and adjusting punishment guidelines for effectiveness and relevance. Ensure transparency and accountability in implementation, providing clear explanations for punishment decisions and establishing mechanisms for review and appeal to address potential biases or errors. Lastly the researcher has discussed the statutory provisions of CrPC, IPC, BNS 2023 and ITA 2000 for C(JI)P Model .

In the digital realm, achieving algorithmic justice requires a delicate equilibrium between compensating cyber victims and penalizing cybercriminals. Cyber compensation algorithms meticulously evaluate the losses suffered by victims, including intangible damages like emotional distress, using data analytics to ensure fair and prompt reimbursement. Simultaneously, the development of cyber insurance calculation algorithms is pivotal in managing financial risks associated with cyber threats, encouraging proactive security measures. These algorithms consider breach severity and future vulnerabilities to tailor coverage options effectively. Conversely, algorithms for punishment must balance deterrence and rehabilitation, drawing from criminology and psychology to assess intent, impact, and recidivism risk. By incorporating factors such as offense severity and criminal history, these algorithms assist judges in imposing fitting penalties that serve both punitive and rehabilitative aims. Transparency and accountability are crucial in algorithmic justice, guaranteeing unbiased sentencing decisions. Through aligning compensation and punishment, algorithmic justice fosters a digital landscape founded on accountability, fairness, and trust

The proposed model integrating safeguarding against cyber threats, risk management strategies, comprehensive compensation, insurance for cyber victims, and punishment for cyber hackers offers several advantages over statutory provisions alone. The integrated model addresses cybercrime mitigation comprehensively, extending beyond punishment and compensation to include proactive risk management and victim support through insurance. Its structured algorithm considers crime severity, damages, victim vulnerability, and perpetrator culpability, enabling nuanced responses.This goes beyond mere compensation mandated by statutory provisions, providing financial protection and assistance to victims in navigating the aftermath of cyber incidents. The combination of comprehensive compensation, insurance, and punishment serves as a stronger deterrent against cybercrimes compared to punishment alone. Potential perpetrators are not only deterred by the threat of legal consequences but also by the prospect of financial liability and the likelihood of being held accountable through insurance mechanisms.

8.2 Future Research Directions

In the rapidly evolving landscape of cybercrimes, where new methods and technologies constantly emerge, determining CRM4 and (C(JI)P Model not explicitly covered by existing cyber laws presents a challenge. In such cases, the judiciary often relies on principles of legal interpretation, precedents from similar cases, and the overarching objectives of the legal system, such as protecting individuals' rights and maintaining societal order. Additionally, legislative bodies may periodically amend existing laws or enact new ones to address

emerging cyber threats, providing legal frameworks for adjudicating these cases. Moreover, judicial discretion allows for flexibility in sentencing, enabling judges to consider the unique circumstances of each case and tailor punishments accordingly, thereby striving to uphold justice in the face of evolving cyber threats.
The implementation of proposed CRM4 and (C(JI)P model combines the notion of safeguarding against cyber threats with risk management strategies, comprehensive compensation, insurance for cyber victims, and punishment for cyber hackers, hence the proposed algorithm for the calculation of compensation, insurance and punishment shall act as a Intelligent Software tool in cybercrime compensation, insurance and punishment decision making process.
There must be a separate clause for The insurance for cyber risk in Bharatiy Nyay Sahita 2023 and IT Act based on the proposed algorithms. The proposed model offers a more robust and adaptive approach to addressing cybercrimes, leveraging a combination of legal, financial, and risk management strategies to enhance cyber resilience and protect victims' interests more effectively than statutory provisions alone.

REFERENCES

[1] Dr. Gupta and Agarwal, Cyber Laws, Premier Publishing Company, 2023
[2] Dr. Santosh kumar, Cyber laws and crimes, Whitesmann Publishing Company, 2nd edition 2022
[3] G.C.Ramamurthy and Kogent Learning Solutions Inc., Research Methodology, Dreamtech press,2015
[4] Piyush Gupta, An Efficient Classifier for U2R, R2L, DoS Attack. International Journal of Recent Technology and Engineering (IJRTE), 2020. A1942059120.pdf (ijrte.org)
[5] Dr.Bandu B. Meshram Dr. Manish Kumar Singh ,Strengthening India's ITA 2000 Cyber Law: Proposed Amendments To Combat Next-Generation Cyber Crimes, International Conference On Navigating Emerging Cybercrime Threats & Enhancing Cybersecurity Measures: Charting The Path Ahead" St 1 June 2024 , Saveetha School of Law (SSL), Saveetha Institute Of Medical And Technical Sciences, Chennai, Tamilnadu, India in collaboration of ASIAN School of cyber Laws and International Institute of justice and police sciences.
[6] NSL-KDD, "NSL-KDD data set for network-based intrusion detection systems," http://iscx.cs.unb.ca /NSL- KDD/, March 2009.
[7] Smitha Rajagopal, Poornima Panduranga Kundapur, and Katiganere Siddaramappa Hareesha, A Stacking Ensemble for Network Intrusion Detection Using Heterogeneous Datasets, Hindawi Security and Communication Networks Volume 2020,
[8] Roger Pressman and Bruce Maxim,Software Engineering: A Practitioner's Approach, 9th Edition, MCgraw- Hill International Edition , 2020
[9] Ramez Elmasri, Shamkant B. Navathe,Fundamentals of Database Systems 7thEdition, pearson/ADDISON Wisley , 2015
[10] Thomas H. Cormen etal." Introduction to algorithms, Fourth edition, Cambridge, Massachusetts : The MIT Press, [2022]
[11] Study Notes of PG Cyber Security Course " Cyber Security & Executive Strategy ,Stanford Centre of Professional development, USA, Copyright © 2017 Stanford University
[12] Bandu B. Meshram,Manish Kumar Singh, Guarding The Digital Cyber Realm Of India: Navigating IPC 1860, Bharatiya Nyaya Sanhita 2023 and ITA 2000 in the Fight Against Cyber Crime, IJRDO - Journal Of Law and Cyber Crime,Volume-3 , Issue-2 , February, 2023
[13]Joey Hernandez,The Cyber Insurance Survival Guide:: Expert Strategies for Preparing and Responding To Cyber Insurance Applications, Independently published (January 3, 2023)- ISBN-13 : 979-8372403062
[14] Gerardus Blokdyk ,Cyber Insurance A Complete Guide, 2020 Edition, 5STARCooks (Feb. 22, 2021)
[15]Prof Philip M. Parker , The 2023-2028 World Outlook for Cyber Security Insurance, ICON Group International, Inc. (May 10, 2022)
[16]IN INADEQUACIES IN BREACH INSURANCE COVERAGE: A DATA-DRIVEN GAP ANALYSIS: HTTPS://CYESEC.COM/RESOURCES/GUIDES-EBOOKS/INADEQUACIES-IN-BREACH-INSURANCE-COVERAGE-A-DATA-DRIVEN-GAP-ANALYSIS
[17]Closing the Cyber Insurance Gap 2023 State of Cyber Insurance Report: https://delinea.com/hubfs/Delinea/whitepapers/delinea-wp-2023-state-of-cyber-insurance-report.pdf
[18] B. B. Meshram, Ms. K.A. Shirsath , TCP/IP and Network Security, Shroff Publishers 7 Distributors Pvt, Ltd. Mumbai feb 2018, ISBN Number 978-93-5213-355-0
[19]W. Stallings, Network Security Essentials - Applications and Standards, Prentice-Hall, Englewood, 2018
[20]. Bandu B. Meshram,Manish Kumar Singh, Guarding The Digital Cyber Realm Of India: Navigating IPC 1860, Bharatiya Nyaya Sanhita 2023 and ITA 2000 in the Fight Against Cyber Crime, IJRDO - Journal Of Law and Cyber Crime,Volume-3 , Issue-2 , February, 2023
[21] National Cyber Crime Research & Innovation Centre (NCR&IC), Report Emerging Cyber Crimes in India: A Concise Compilation: http://bprd.nic.in/uploads/pdf/ 202204050353115253612Emerging CyberCrimesinIndia.pdf
[22] Fifth-generation cyber-attacks are here. How can the IT industry adapt? Feb 12, 2021

https://www.weforum.org/agenda/2021/02/fifth-generation-cyberattacks/
[23] B B Meshram Interview: Bitcoin crypto currency: cyber-attack:
:https://www.etvbharat.com/Marathi/Maharashtra/state/Mumbai/adeven-of-the-bitcoin-cryptocurrency-has-made-finding–cberattackers-more-dificult-vjti-expert-claims/mh20221127141821570570388
[24] National Cyber Crime Research & Innovation Centre (NCR&IC) Report Emerging Cyber Crimes in India: A Concise Compilation: http://bprd.nic.in/uploads/pdf/ 20220405035311525361 2Emerging CyberCrimesinIndia.pdf
[25] National Cyber Crime Research & Innovation Centre (NCR&IC) Bureau Of Police Research And Development Ministry Of Home Affairs, Government Of India Nh-8, Mahipalpur, New Delhi-11003
"National Level Webinar on Cyber Security Preparedness for Next 10 Years" : chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://bprd.nic.in/uploads/pdf/20220607022338330 7279NationallevelWebinaronCy.pdf
[26]National Cyber Crime Research & Innovation Centre (NCR&IC) Bureau Of Police Research And Development Ministry Of Home Affairs, Government Of India Nh-8, Mahipalpur, New Delhi-11003
Emerging Cybersecurity Challenges, June 30, 2021:
/https://bprd.nic.in/uploads/pdf/202206070223383307279NationallevelWebinaronCy.pdf
[27] Bandu B. Meshram,, Vikash Mendhe ,, Manish Kumar Singh, Tracing the Invisible Threads: A Deep Dive into Email Security & Forensics , International Journal of Enhanced Research in Science, Technology & Engineering, ISSN: 2319-7463, Vol. 13 Issue 1, January-2024, https://www.erpublications.com/uploaded_files/download/bandu-b-meshram-vikash-mendhe-manish-kumar-singh_BRQtv.pdf
[28] Madhuri N. Gedam and B. B. Meshram, Database Private Security Jurisprudence: A Case Study Using Oracle , International Journal of Database Management Systems (IJDMS) Vol.13, No.3, June 2021
[29]Dinesh N Patil, Bandu B Meshram, Web browser analysis for detecting user activities Recent Findings in Intelligent Computing Techniques: Proceedings of the 5th ICACNI 2017, Volume 1 279-291,Publisher ,Springer Singapore, 2019
[30] Criminal Procedure code 1973, Bare Act, 2019
[31]Information Technology Bare Act 2000/2008,
[32] Bharatiya Nyaya Sanhita 2024 Bare Act, Professional book Publisher.
[33]The Indian Penal Code, Bare Act 2019
[34] The Bharatiy Nagrik Suraksha Sanhita, 2023 .