Cognitive Computing and Cybersecurity Threat Mitigation: A Strategic Framework for Organizational Resilience

Mridul Bhattacharjee , Syed Athif Usma , Mohamed Muzni Mohamed Ziham , Rozin Khan , Muhammad Shabir Abdul Razick , Noor Ul Amin *

Posted Date: 30 April 2025

doi: 10.20944/preprints202504.2532.v1

Keywords: organizational resilience; cybersecurity; cyber threats; cognitive computing; IBM Watson

 doi:10.20944/preprints202504.2532.v1

Article

Cognitive Computing and Cybersecurity Threat Mitigation: A Strategic Framework for Organizational Resilience

Mridul Bhattacharjee, Syed Athif Usman, Mohamed Muzni Mohamed Ziham, Rozin Khan, Muhammad Shabir Abdul Razick and Noor Ul Amin *

Taylor's University

* Correspondence: nooraminnawab@gmail.com

Abstract: Cyber spacing being harnessed as a foundation for global development and financial systems has posed increasing threats to organizational stability, compliance with regulations, and integrity of data. The report employs a two-pronged approach: firstly, assessing all threats and creating an organizational taxonomy for XYZ Company and getting into the details of vulnerabilities and trends of cyberattacks with the support of case studies like the Snowflake data breach and the Salt Typhoon campaign. Included here are ransomware, phishing, DDoS, and advanced persistent attacks. Secondly, an evaluation of how the implementations of cognitive computing platforms in IBM Watson and Palantir Foundry may mitigate financial risks arises. By contrasting their predictive analytics, compliance automation, capabilities for integration, and limitations, the research pinpoints the desirable context for each system deployment in the Malaysian regulatory environment. The analyses highlight the need for a multi-layered cybersecurity approach that embraces AI-driven solutions, employee training, and real-time detection of threats to guarantee the operational resilience of organizations while nationally aligning data protection efforts.

Keywords: organizational resilience; cybersecurity; cyber threats; cognitive computing; IBM Watson

1. Introduction

As organizational sustainability and national security are aided by the advent of the cyber age, so are these new technologies making their way into the organizations with the adoption of cloud computing, artificial intelligence, and data-driven systems, therefore extending and complicating the threat landscape. Cybercrime has transformed from isolated incidents into something that emerges throughout the world with economic consequences. In the estimation of Cybersecurity Ventures, the global cost of cybercrime is projected to reach $10.5 trillion per annum by 2025, as against $3 trillion in 2015, emphasizing the pressing need for transforming cyber defenses [1–4]. This challenge pertains very much to organizations that try to incorporate the Sustainable Development Goals (SDGs) of the United Nations, where digital resilience is necessary for their attainment, such as for the eradication of poverty, promotion of quality education, and reduced inequalities. Nevertheless, the frequent and highly sophisticated cyberattacks, including ransomware, phishing, distributed denial-of-service (DDoS), and advanced persistent threats (APTs), impede security and operational continuity of these very objectives. Moreover, the increasing reliance on digital infrastructures warrants not just technical security measures but also strategic frameworks whose objective is the proactive management of risk [5–8]. Cognitive computing platforms such as IBM Watson and Palantir Foundry have come to be very powerful in improving the state of readiness in cybersecurity and in securing financial risk management. In these systems, AI, machine learning, and big data analytics are getting used to detect anomalies, predict threats, and ensure compliance with regulations. When such platforms or technologies are brought in as part of the ecosystem of the organizations, adaptive responses to cyber threats can be effected in real-time, meaning decreased levels of vulnerabilities

 doi:10.20944/preprints202504.2532.v1

and improved levels of resilience. The main target of this paper is to study current cyber threats, examine their influence on organizational security, and to evaluate the functionality of cognitive computing systems in risk mitigation from the viewpoint of financial and strategic management of XYZ Company [9–14].

Figure 1. indicates the trends in the most common prevention methods for popular types of cyber-attacks [15].

Indeed, it goes far beyond common criminals and state-sponsored enemies. In 2023, an average of 7.65 attacks hit a company every week, and it is estimated that in 2024 the global average cost of cybercrime will reach $9.5 trillion. Ransomware is a serious danger that can run a business into a lot of trouble financially. 74% of breaches result from human error; thus, security awareness training is necessary [16–20]. AVOIDIT (a Taxonomy of cyberattacks), is currently used to categorize and carry out an understanding of cyber-attacks. Specifically, it establishes defensive tactics based on specific vulnerabilities discovered in the taxonomy and enhances the skill of network administrators in improving network security by classifying threats with repair methods [47–49]. The taxonomy is well structured to classify blended attacks and also provides a knowledge repository for defenders to understand and mitigate cyber threats [50–52].

2. Literature Review

Emerging sophistications in cyber threats alongside their increasing occurrences have necessitated the adoption of technologically advanced solutions such as cognitive computing within modern organizations. Literature underscores the urgency to reinforce digital infrastructures, especially in critical sectors like finance, health sector, and government, as breaches in these sectors have significant consequences [21,22].

Recent studies emphasize diverse manifestations of cyber threats, ranging from ransomware, phishing attacks, distributed denial-of-service (DDoS) attacks, and advanced persistent threats (APTs). Particularly, ransomware attacks have proven most destructive through encryptions with demands for ransom payments, often running down sectors like [23]. The obvious few attacks include the 2024 Snowflake breach and the Change Healthcare ransomware attack, highlighting the vulnerability of such systems to credential theft alongside exploitation from cloud-based services [24–27].

State-sponsored cyber-espionage campaigns, like China's Salt Typhoon operation and cybercriminals associated with North Korea, specify the geopolitical dimension of security threats. Most of these attacks deploy social engineering methods, phishing attacks, or vulnerability any kind of software provides for users to get into a system and extract sensitive data [28–30]. To analyze and respond effectively to the various cyber threats, cyberattack taxonomies such as AVOIDIT provide structured classifications [31,32]. But, unfortunately, 74% of breaches have been attributed by reports to user error, indicating the human factor still alive despite the availability of the frameworks [33–35].

Organizations will increasingly use cognitive computing systems powered by AI, ML, and big data analytics to empower risk prediction and risk-based decisions so that they can help mitigate

 doi:10.20944/preprints202504.2532.v1

emerging risks. It processes large amounts of structured and unstructured data, detects anomalies, and extrapolates predictive insights as regards financial and operational risks [36–38].

IBM Watson is among the leading platforms for integrating ML with natural language processing to detect fraud, automate compliance, and contrast credit risks. Among the case studies available, Citibank and Standard Chartered have used Watson to minimize fraudulent transactions in real-time while complying with regulatory requirements from various jurisdictions [39]. High implementation costs and customization issues can curb its application use [40].

In contrast, Palantir Foundry offers robust data integration capabilities and is suited for large-scale risk analysis; its real-time monitoring, predictive modeling, and fine-grained access controls cater to environments where security is paramount, such as government defense agencies and large financial institutions [41–44]. However, it also puts high demands on technical infrastructure and has a steep learning curve, especially in integrating with legacy systems (Launch Consulting, n.d.) Comparatively, one source states that, while IBM Watson shines in the space of fraud detection and NLP-based compliance analysis, Palantir Foundry is potent on data integration and real-time risk tracking, making it more suited for large banks and regulatory agencies in Malaysia-Malaysia Registry Act, 2023 such as Maybank and Bank Negara Malaysia. For fintech startups and mid-tiers, IBM Watson presents a tailored and scalable fraud detection solution. Both platforms use automation and advanced analytics to ensure regulatory compliance under the Personal Data Protection Act (PDPA) and Basel III standards with stringent data governance measures [45–47].

3. Methodology

The analysis was qualitative in nature, involving document analysis, case study evaluation, and comparative assessment. The methodology was distilled into two main steps: The first step consisted of an extensive review of the secondary data sources, including academic articles, media reports, cybersecurity frameworks, and white papers in technology, among others. Key sources consulted were the AVOIDIT taxonomy for cyberattack classification; the actual-world reports, by IBM and Palantir; and some guidelines and regulations from government and official organizations, such as Bank Negara Malaysia and FATF. Such events as the 2024 Snowflake data breach, the Change Healthcare ransomware attack, and the state-sponsored Salt Typhoon campaign were analyzed to learn about the nature, tactics, and consequences of modern threats [53–55].

The second phase of methodology concerned the thematic content analysis of these incidents and mitigation strategies. A taxonomy-based organizational model from which to map relationships between various departments, assets, and cybersecurity functions in XYZ Company was designed and further represented by a UML diagram and structured relational table to denote associations and generalizations. At the same time, two cognitive computing platforms—IBM Watson and Palantir Foundry—were assessed by a comparative framework focusing on their functionality, strengths and weaknesses, and appropriateness for Malaysian financial institutions [56].

Hill charts, figures, and tables facilitated by Python-based data analysis tools (Google Collaboratory, etc.) were fabricated [57], guided by the insights obtained from the documented cases and system specifications. Emphasis was further placed on real applicability with solutions mapping onto the company's departmental set-up, regulatory requirements, and known vulnerabilities, ensuring that the solutions proposed are indeed operationally present.

4. Cybersecurity Measure Implications

Strong security controls and cybersecurity training for employees are essential given the rising number of confirmed and suspected credential compromises [58,59] and their unmistakable link to attack success. Companies may need to ramp up their vulnerability management initiatives, tighten authentication procedures, and utilize continuous monitoring.

Table 1. Summary Table of each resource tackling general attack types.

 doi:10.20944/preprints202504.2532.v1

Source/Participant	Focus	Approach/Style	Emphasis
TechTarget Article	Detailed types & prevention of cyberattacks	Structured list, case studies	Practical measures, real-world examples
Geeks for Geeks Article	Overview of cybercrime and its impacts	Educational, overview-based	Definitions, legal aspects, basic prevention
Academic Paper (AVOIDIT Taxonomy)	Systematic classification of cyber attacks	Technical, research-oriented	In-depth taxonomy with multiple dimensions
Narrative/Case Study Video Transcripts	Step-by-step account of multi-stage attacks	Conversational, storytelling	Realistic depiction of attack progression

Finally with the sources identify malware (specifically ransomware), phishing, password attacks, DDoS, and injection attacks (SQL injection and XSS) as being among the most common forms of cyber-attacks. Various facts—such as the fact that there are an enormous number of attacks per week per organization, mean breach costs, and how important stolen credentials are to show that these are the most insidious threats to modern organizations and systems.

4.1. Overview of the Most Frequent Kind of Cyberattacks

The mentioned types of cyberattacks are oftentimes discussed and regularly seen, according to the source documents:

1. Ransomware: Extorts payment upon encrypting the victim's data. Trojan horses, rootkits, and spyware are evil programs which pose as beneficial ones.
2. Phisher attacks: Spear phishing, whaling, and business email compromise (BEC) are methods of attack used to target emails in order to obtain sensitive data, such as login credentials.
3. Password attacks: Sniffing, dictionary, brute-force, and keylogging are methods of obtaining unauthorized access via exploiting weak or reused passwords.
4. Distributed Denial-of-Service (DDoS) attacks: Hundreds of millions of requests overwhelm network capacity, leaving legitimate users unable to utilize services. Injection attacks
5. Trojan code: can be injected into web applications using SQL Injection and Cross-Site Scripting (XSS) vulnerabilities.
6. Man-in-the-Middle attacks: intercept and alter two people's conversations without either's awareness.

4.2. Overview of Prevention Strategies

Table 2. Overview of prevention strategies.

Attack Type	Key Prevention Strategies
Malware /Ransomware	Antivirus/anti-malware, email filtering, patch management, secure backups, user awareness

 doi:10.20944/preprints202504.2532.v1

Password Attacks	Strong password policies, MFA, account lockout, regular password updates, user training
DDoS Attacks	Traffic filtering, rate limiting, load balancing, DDoS mitigation services, network segmentation, continuous traffic monitoring
Phishing Attacks	Email authentication (SPF/DKIM/DMARC), anti-phishing tools, browser security alerts, employee training
SQL Injection	Input validation, parameterized queries, code reviews, least privilege, WAFs
Cross-Site Scripting	Output encoding, input sanitization, CSP headers, regular security testing
Man-in-the-Middle	End-to-end encryption (SSL/TLS), VPN deployment, mutual authentication, network segmentation, certificate management

Ransomware, SQL Injection, and MITM are the most severe types of attacks due to the fact that they cause irreversible data loss, financial damage, and business interruption. Phishing, Password Attacks, and DDoS are the easiest attacks for hackers and, thus, the most common ones. They seldom require any sort of technical expertise but can still successfully produce serious consequences. Some of the costliest attacks to recover from are Ransomware attacks, DDoS attacks, and SQL Injection attacks. Malware that does this leaves serious downtime, legal penalties, and high costs of recovery. Of these, DDOS attacks are easy for the non-technical attacker, very hard to trace, not quite heavy enough to warrant serious countermeasures, and too painful to recover from financially; hence we can state that DDoS attacks are the worst type of cyber-attack.

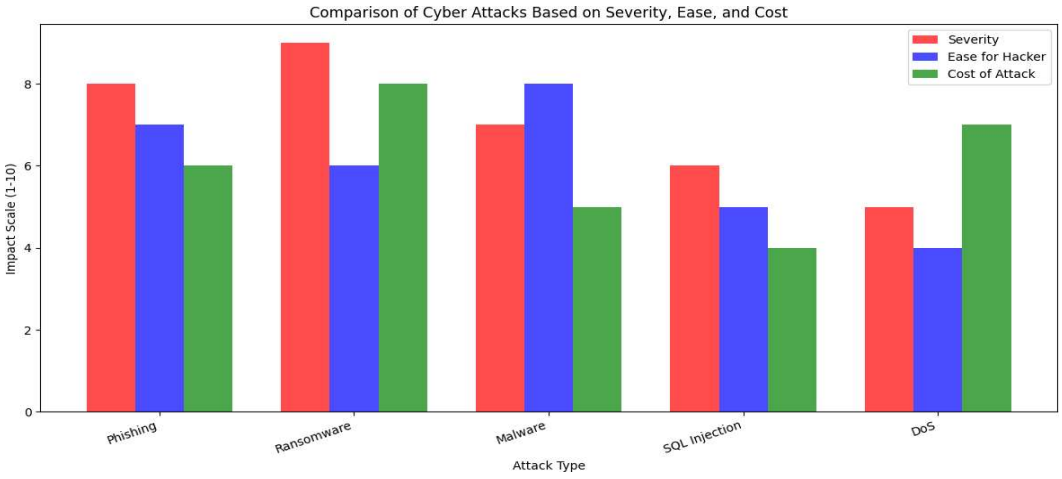


Figure 2. Comparison of Cyber Attacks in terms of Severity, Ease and Cost (Created in python via using insights extracted from sources by analysis tools).

These forms of malware and ransomware could cripple the functioning of an entire organization by encrypting critical files and demanding a hefty ransom for unlocking those files. Distributing these malevolent distractive programs could be achieved via phishing emails, infected websites, or by malicious downloads, thereby resulting in ransom payoffs, operational downtimes, extensive recoveries, and even huge reputational damage. Password attacks include brute-force attempts,

 doi:10.20944/preprints202504.2532.v1

credential stuffing, and phishing attacks, which are posing yet another serious threat because they facilitate unauthorized access, data theft, and identity fraud. An attack that does not involve physical intrusion is relatively easy to perpetrate, and recovery costs the victim severely depend upon sensitivity and accessibility of the compromised data.

Distributed denial of service (DDoS) attacks is one of the most potent threats to websites, services, or even an entire network because they overwhelm a target with traffic, usually from botnets and amplification techniques. An attack just like this may cause a company to go offline temporarily, directly resulting in revenue loss and possible physical damage to infrastructure. Phishing attacks still remain in the same category; they rely on the social engineering technique in persuading their victims to unknowingly reveal their credentials or financial account information to them, which is then subsequently used to further many other criminal acts like identity theft, financial fraud, malware infections, and penalties imposed for regulatory compliance failure. Such SQL Injection attacks typically destroy or at least expose total databases, giving ample opportunity for losing data, regulatory fines, and compliance violations. Poorly sanitized input allows the attacker to inject scripts into web applications; in this nature similar to SQL injection is cross-site scripting (XSS), where those injected scripts allow the attacker the ability to steal session data or redirect the user to malicious sites, but generally does not paralyze system-wide affairs. Finally, we have the critical threat of Man-in-the-Middle (MITM) attacks, intercepting and possibly altering communications between parties. Such breaches are usually beyond recovery and cause stolen credentials, financial losses, and compromised business communications.

4.3. Specified Dangerous Cyber-Attacks That Took Place in Recent Times

The same is the case or rather they deal with all the four main departments in the company: marketing, finance, cybersecurity, and computer systems within the organization, thereby being involved at a corporate level. Knowledge of the integrated cyber-attacks that are occurring in the present times is useful when it comes to improving the defense line securing the private information of the institution. Some very vital cyber events illustrate how the scenario is constantly changing.

The first major incident is the Snowflake data breach of 2024, in which users of this cloud platform were targeted. Stolen user credentials were used for illegal access causing a serious breach that exposed sensitive customer information. The event is said to be serious for those organizations affected, with heavy financial losses as well as loss of reputation, thereby proving the risks of loose credential protection and mismanagement of cloud security [44].

Another critical event included the ransomware attack on Change Healthcare in 2024. Cyber attackers exploited vulnerabilities in the company's IT infrastructure, bringing about unprecedented service disruptions, disruption of patient care, loss of data, and significant financial loss [45]. The event is noteworthy as it necessitates system monitoring in real-time and regular software updates in a bid to prevent ransomware attacks.

The third is the Salt Typhoon campaign, a state-led Chinese cyber-espionage campaign against key infrastructure since 2012. Phishing campaigns and advanced persistent threats (APTs) were used by Salt Typhoon to obtain access into government and telecommunications networks across the globe, exposing private data at risk and representing a significant national security threat. The attack highlights the need for improved email security and threat intelligence controls [46].

The third attack involves North Korean cyber gangs that have been behind many politically and financially motivated cyberattacks. The cyberattacks were mainly against financial institutions and cryptocurrency exchanges, causing financial instability and raising global tensions by evading sanctions and supporting illegal activities. This attack shows the greatest necessity for efficient fraud detection systems and regulation of financial transactions.

4.4. Comparative Analysis of Cyber-Incidents

An overview of comparative cyber-incidents in the year 2024, focusing on some attacks initiated by hacker groups from North Korea, such as Snowflake and Change Healthcare, and the Salt

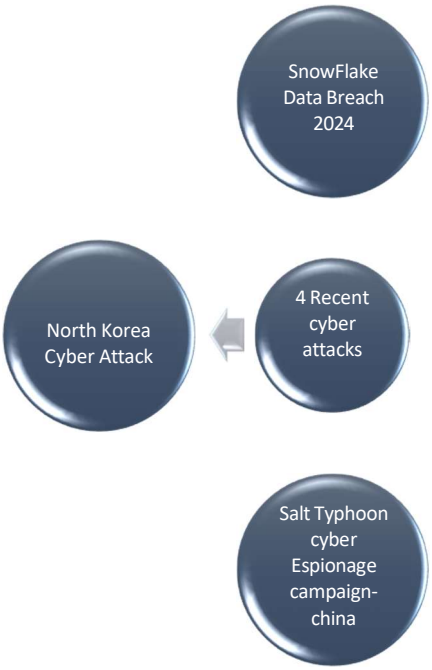
 doi:10.20944/preprints202504.2532.v1

Typhoon campaign, demonstrates how quickly and destructively modern cyber-targeting has become. All the incidents affecting Snowflake and Change Healthcare were ransomware attacks and data leaks that paralyzed their various operations and, notwithstanding, exposed sensitive information. In general, North Korean hackers and Salt Typhoon have remained focused on targeting financial theft and cyber-espionage activities.

Primary attack vectors for the Snowflake and Change Healthcare breaches included the following: compromised credentials and IT system vulnerabilities, which together culminated in unauthorized encryption and access of critical data. Differently, North Korean and Salt Typhoon hackers relied on such fail-proof phishing attacks, "advanced persistent threats," and covert "living off land" techniques to infiltrate networks without detection. Prominently, Salt Typhoon focused on intelligence gathering by exploiting software vulnerabilities in critical infrastructures. By this, the consequences of these attacks have been harsh. One of the bangs shattered by the Snowflake breach concerns exposing the vulnerability of cloud security. It was disruption to healthcare services and huge financial costs that the great change caused for Change Healthcare. National insecurity in the Salt Typhoon campaign was compromised because sensitive government data leaked. North Korean attacks have further destabilized financial systems through cryptocurrency thefts.

4.5. Concerned Recommendations for Safeguarding XYZ Company from Cyber Threats

It will require a catch-all, multi-layered cybersecurity strategy for all departments—marketing, finance, cybersecurity, and computer-to protect XYZ Company against emerging cyber threats. Such departments should at least implement Zero Trust Architecture, which strictly enforces verification for any access requests before granting approval. The computer and cybersecurity teams shall employ robust multi-factor authentication (MFA) to ensure prevention of credential theft similar to the Snowflake incident. This will include the deployment of AI-enabled endpoint protection systems by the cybersecurity department to enable the systems detect unusual behavioral changes in real time, thereby capturing ransomware or APT activity before it worsens. Conduct regular security audits followed by the speedy patching of vulnerabilities, especially against weaknesses that are exploited in incidents such as Change Healthcare's attack. In addition, programs on phishing awareness should be conducted to train all workers especially in the marketing and finance departments on social engineering attacks such as used in Salt Typhoon campaign. Tight network segmentation and access controls will restrict lateral movement in the hypothetical event of compromise, ensuring that each department has access only to the data they need.



 doi:10.20944/preprints202504.2532.v1

Figure 3. Recent cyber-attacks globally.

There needs to be deployment of threat detection and behavioral analytics systems within the finance department that have the capability to detect abnormal financial transactions and prevent cryptocurrency thefts such as those conducted by North Korean hackers. To ensure that sensitive data is secured even in the event of a breach, data encryption and regular secure backups must be rendered mandatory in all critical systems. Lastly, XYZ Company must have a thorough incident response plan in place to contain and recover from cyber incidents quickly, with minimal disruption and organizational continuity. With these proactive and multi-layered cybersecurity measures, XYZ Company can more effectively protect itself from an ever-evolving hostile digital threat environment.

4.6. Organizational Taxonomy for XYZ Company

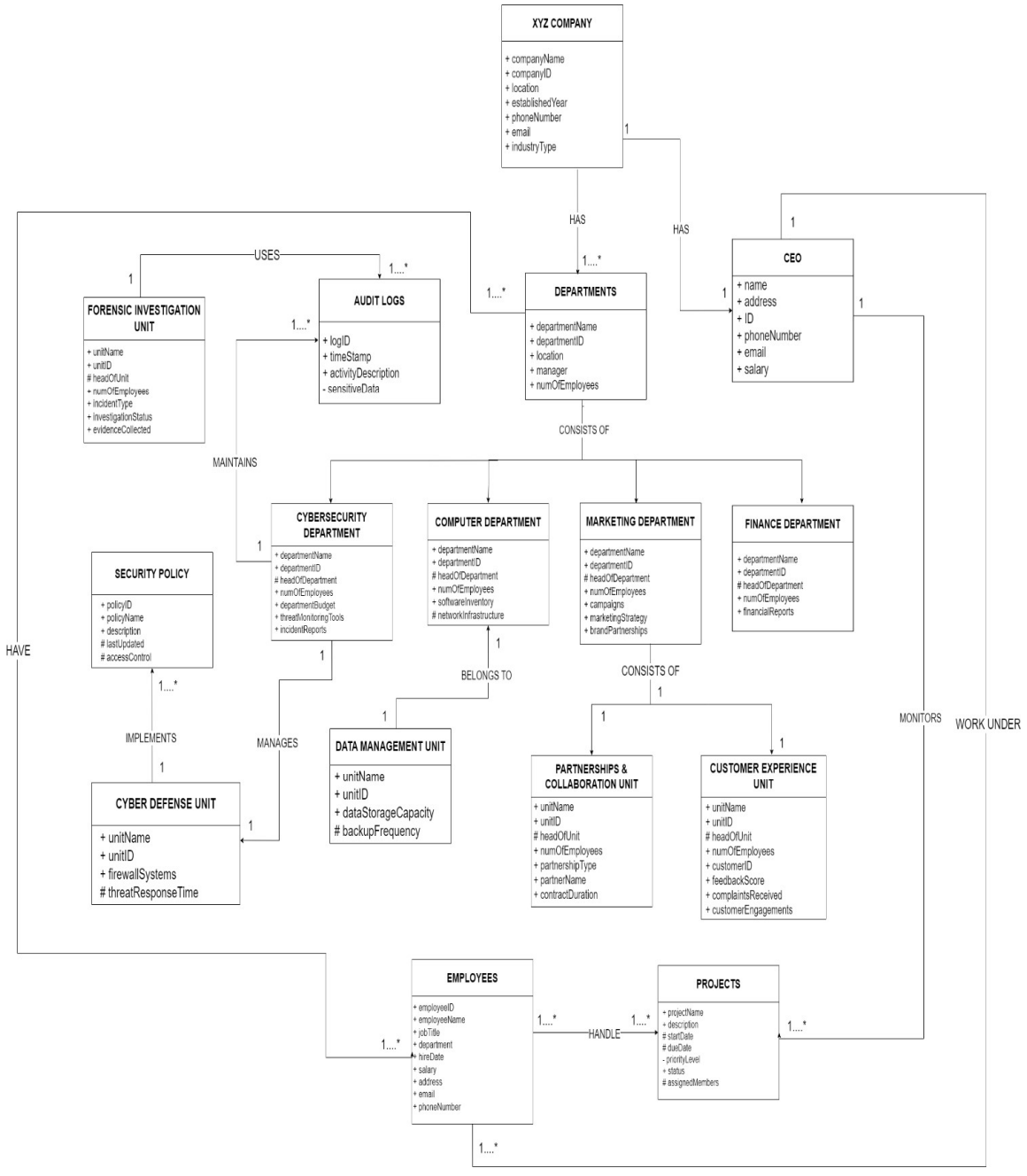


Figure 4. UML Diagram for XYZ company.

 doi:10.20944/preprints202504.2532.v1

4.7. Organizational Taxonomy for XYZ Company

The XYZ Company is structured into four primary departments: Computer, Cybersecurity, Finance, and Marketing. The departments are all crucial in helping the company achieve its objectives while facilitating operational efficiency. The company utilizes a taxonomy approach to guarantee a well-defined representation of the hierarchical structure, illustrating relationships, attributes, and associations among the different components within the company. A detailed explanation of the taxonomy is given below:

4.8. Explanation of the Concepts and Relationships

Company and Departments (Association):

The XYZ Company is composed of several departments, each managing distinct operations. The relationship is classified as an association, indicating that departments are essential structural components of the company.

4.9. Departments and Corresponding Departments (Specialization)

The departments are divided into four distinct categories: Computer, Cybersecurity, Finance, and Marketing. The relationship is defined as specialization, meaning that each department is a more specific version of a general category within the company's organizational hierarchy.

4.10. Departments and Employees (Association)

Employees are associated with specific departments, signifying that each department comprises multiple employees who are responsible for handling various projects and operational activities.

4.11. XYZ Company and CEO (Association)

The CEO holds an associative relationship with the entire company, overseeing all departments and leading strategic decision-making processes.

4.12. CEO and Projects (Association)

The CEO is in an associative relationship with company projects, always monitoring progress so that it is aligned with corporate goals and objectives.

4.13. Employees and Projects (Association)

The employees are held directly responsible for executing projects and making contributions to successful project implementation.

4.14. Employees and CEO (Association)

The employees are overseen by the CEO, where their contributions are aligned with the general organizational strategies and project requirements.

4.15. Data Management Unit and Computer Department (Association)

The Data Management Unit is located in the Computer Department and is tasked with conducting operations such as data storage, processing, and retrieval.

4.16. Relationship Between Cybersecurity Department and Audit Logs

Audit logs are important to monitor security-related activities. The Cybersecurity Department is responsible for updating and reviewing these logs to enhance the cybersecurity position of the organization.

 doi:10.20944/preprints202504.2532.v1

4.17. Relationship Between Cybersecurity Department and Cyber Defense Unit

Cyber Defense Unit is a mission-critical sub-unit of Cybersecurity Department whose responsibility is deployment of defensive countermeasures to cyber-attacks and threats.

4.18. Security Policy (Association) and Cyber Defense Unit

Security policies, established and regulated by the Cyber Defense Unit, govern access to data and systems to ensure confidentiality, integrity, and security from potential damages.

4.19. Forensic Investigation Unit and Audit Logs (Association)

The Forensic Incident Investigation Unit investigates cyber violations via the process of gathering information electronically and relies massively on audit logs to keep an eye on patterns, follow security breaches, and assist the law enforcement authorities.

4.20. Marketing Department and Partnerships & Collaboration Unit (Specialization)

Partnerships & Collaboration Unit is a specialist marketing department unit engaged in forging relationships with foreign organizations, corporations, and government agencies to facilitate the development of the firm's reputation along with increasing its horizon of market share.

4.21. Marketing Department and Customer Experience Unit (Specialization)

The Customer Experience Unit, again under the Marketing Department, is responsible for increasing customer engagement by understanding and meeting customer needs and expectations.

This categorization enables an integrated understanding of how different things—departments, employees, projects, and security measures—collaborate with one another. Embracing this organized strategy, XYZ Company can more effectively be able to control resources and safeguard data and operations from likely cyber-attacks.

4.22. Cognitive Computing for Enhanced Risk Discovery in LRMC

Cognitive Systems for Financial Risk Management: Overview

Cognitive systems are leveraging Artificial Intelligence (AI), Machine Learning (ML), and Big Data analytics to power operations in the financial services sector. Cognitive systems play a pivotal role in risk detection, predictive analysis, regulatory compliance, and improving overall decision-making processes. With the examination of massive amounts of structured and unstructured historical data, cognitive systems provide recommendations and predictions that help financial institutions reduce fraud, credit risk, and operational inefficiencies. As cyber-attacks and frauds get more advanced, the requirement for cognitive systems becomes more essential. AI and Big Data analytics supported by cognitive computing are most likely to play an important part in future financial risk management. Among the most advanced cognitive solutions, IBM Watson and Palantir Foundry stand out due to their robust infrastructure, verification capabilities, and eco-friendly measures.

4.23. IBM Watson: Finance-Driven Risk Management Through AI

IBM Watson is a robust AI-powered cognitive computing platform developed by IBM to assist organizations in handling risk and compliance with regulatory requirements. IBM Watson uses ML and Natural Language Processing (NLP) to analyze structured and unstructured financial data like risk reports, regulatory reports, and historical case studies to generate actionable insights into risk management (IBM, n.d.). It has been widely utilized by financial institutions to address fraud detection, credit risk assessment, and regulatory compliance issues and therefore is a highly relevant solution for improving financial risk management practices in Malaysia.

 doi:10.20944/preprints202504.2532.v1

4.24. IBM Watson Capabilities for Risk Management

AI-Powered Risk Insights:

IBM Watson applies ML and NLP to process large financial data sets to identify early warning signals of risk. For example, CitiBank uses Watson to scan millions of transactions and detect fraudulent transactions in real-time, enabling proactive risk mitigation.

4.25. Automated Compliance Management

Watson governs and monitors adherence to financial regulations such as Basel III, IFRS 9, and Anti-Money Laundering (AML) regulations. HSBC has integrated Watson to simplify monitoring of compliance processes for automation, reducing manual workloads and enhancing regulatory compliance, particularly in Bank Negara Malaysia's system.

4.26. Predictive Analytics

IBM Watson's predictive analytics capabilities examine credit risks, market volatility, and fraud trends. BNP Paribas leverages these capabilities to examine lending risks and support financial decision-making processes.

4.27. Cognitive Automation:

Watson performs tasks such as policy assessment, fraud detection, and risk analysis. For example, ANZ Bank employs Watson to automate loan application processing, accelerating processing times and boosting operational efficiency.

4.28. Integration Capabilities:

IBM Watson can be seamlessly integrated into existing financial IT infrastructures, including Enterprise Resource Planning (ERP) systems, risk management systems, and regulatory data bases.

4.29. IBM Watson Benefits

Anticipatory Identification of Risk:

Watson empowers banks and financial institutions to recognize risk and act beforehand by means of artificial intelligence-powered analysis. Deutsche Bank utilizes Watson in order to project risks to markets and reallocate investment planning accordingly.

4.30. Deterring Non-Compliance

IBM Watson keeps institutions informed of evolving global and domestic financial rules and regulations and prevents them from incurring legal fines and reputational damage. Standard Chartered Bank uses Watson for AML control in various countries.

4.31. Improved Decision-Making

IBM Watson, on the basis of risk analysis driven by data, enables financial institutions to make highly informed business decisions. For instance, UBS uses Watson to handle client portfolios and tailor investment policies.

4.32. Operational Efficiency

With automation of routine risk assessments and compliance processes, IBM Watson can release human capabilities for value-add activities. Automation of customer service and real-time risk monitoring is employed by DBS Bank in Singapore via Watson to enhance both efficacy and quality of service.

 doi:10.20944/preprints202504.2532.v1

4.33. Limitations of IBM Watson

1. High Implementation Cost: For deploying IBM Watson, there is enormous initial investment in hardware, training the artificial intelligence, and configuring underlying software. Long-term returns made high initial expenditures worth investing in using Watson as a component of JP Morgan's risk management infrastructure.

2. Advanced Customization: In the first place, Watson's AI models can be tailored to particular financial risk scenarios, a time- and resource-consuming activity. To adapt Watson to its (the bespoke) risk assessment needs, Barclays spent months training Watson's AI models.

3. Data Privacy Concerns: For financial institutions, robust data protection compliance takes precedence, similar to in the instance of regulatory frameworks such as Malaysia's Personal Data Protection Act (PDPA), or GDPR. With respect to putting Watson to work with sensitive financial transactions, ING Bank had to introduce added cyber security controls.

4. Reliance on Data Quality: Accuracy and completeness of data significantly influence what IBM Watson will predict or insight into. A problem for Wells Fargo stemmed from missing or contradictory data leading to incorrect risk determinations.

4.34. Palantir Foundry: Extremely Sophisticated Data Integration to Reduce Risk

Palantir Foundry is an analytics and integration platform that is mainly designed to allow organizations to manage complex and large volumes of data, enhancing decision-making process. With the application of artificial intelligence, machine learning and big data tools, this platform forms a strong model to identify, manage and assess the risk. Its predictive modeling algorithm enables the companies to examine their past data and generate future forecasts regarding their steps. This forecasting facility becomes essential in the context of a risk management system for any firm since firms gain their insight and the company's future forecasting due to decisions made. Benefits are real-time risk monitoring system, fraud detection, regulatory compliance among many others. According to the Palantir foundry risk management framework, businesses around the world can enhance their operations efficiency and company's financial stability.

4.35. Palantir Foundry Features for Risk Management

Palantir Foundry has a number of sophisticated capabilities which make it ideal for financial risk management. One of its greatest capabilities is Unified Data Integration, whereby the risk models, transactional data, regulatory reporting, and data sources are all combined on one platform. This integrated approach enhances the pace of risk analysis by allowing for in-depth data visibility and seamless operations. Another key ability is AI-Powered Risk Analysis, whereby the platform uses machine learning and artificial intelligence models to examine historical data, recognize patterns, and uncover potential risks. Foundry also provides detailed reports and actionable recommendations, enabling companies to make informed decisions.

Regulatory Compliance Automation is another key ability, enabling financial institutions to meet requirements under regulations like Basel III, IFRS 9, and Anti-Money Laundering (AML) legislation. With automated compliance tracking, the platform reduces human error and maintains regulatory compliance. Additionally, Palantir Foundry provides Real-Time Risk Monitoring, which helps industries monitor financial market trends in real-time and respond to increasing risks proactively. Further, its Scalable and Customizable Infrastructure enables organizations to tailor risk models and workflows according to individual institutional needs, providing the flexibility necessary for growing and changing infrastructure.

4.36. Benefits of Palantir Foundry

Palantir Foundry offers numerous benefits to organizations looking to improve their financial risk management. A major benefit is Enhanced Risk Identification since the AI-driven analytics allow businesses to spot risks before they happen, and hence safeguard assets and reduce risk exposure.

 doi:10.20944/preprints202504.2532.v1

Better Regulatory Compliance is also facilitated through the platform via auto-enabled processes and reduced risks of breaches and associated legal problems. Another significant advantage is Data-Driven Decision Making, whereby the historic and real-time data available to institutions enables the making of adequately supported, fact-based financial choices.

End-to-End Data Integration and Transformation is a unique advantage as Foundry successfully pulls together structured data and unstructured data from diverse sources and enables consistent operations. Granular Access Control and Data Security is also highly prioritized, with hyper-granular permissions enabling hard controls over access to data as well as how it is processed. Additionally, Foundry contains No-Code/Low-Code Pipelines that allow users who are not technical to construct data transformation flows through simple drag-and-drop interfaces, thereby reducing reliance on technical staff and accelerating operational processes. Lastly, Palantir Foundry is notable for its Military-Grade Security and a Demonstrated Track Record in defense and intelligence organizations, having been broadly utilized by government agencies like the CIA and the U.S. Department of Defense for sensitive missions.

4.37. Limitations of Palantir Foundry

While it is rich in advantages, Palantir Foundry also has some disadvantages. High Implementation and Maintenance Cost is perhaps the largest disadvantage. Its installation, infrastructure, environment, training, and customization are too expensive, restricting the platform primarily to large institutions such as Morgan Stanley and Goldman Sachs, since small companies cannot afford its expense. Another disadvantage is the Complexity of Integration with Legacy Systems. The implementation of Palantir Foundry together with other financial technology infrastructures is cumbersome and challenging, as was the case with the case of UBS that suffered a few months of adaptation challenges.

The platform also exhibits a Steep Learning Curve. Although facilitated by no-code/low-code capabilities, intense customization requires deep technical expertise, thus posing difficulties for risk analysts and financial managers who are non-technical. Lastly, Data Privacy and Regulatory Concerns are major concerns. Because of the sensitive financial data handled by Foundry, institutions such as Credit Suisse have been forced to employ additional encryption and cybersecurity to meet stringent regulatory standards such as GDPR, PDPA, and Basel III compliance.

5. Conclusion

This report has explored the double dimension of cybersecurity threat management and cognitive computing implementation for risk prevention in XYZ Company. Through rigorous threat analysis and taxonomy modeling, it is apparent that modern-day organizations are faced with a wide array of cyberattacks—from ransomware and phishing to state-sponsored espionage. A multi-layered cybersecurity model comprising prevention, detection, response, and recovery is essential. Concurrently, financial risk management can be revolutionized using cognitive computing platforms such as IBM Watson and Palantir Foundry through the delivery of AI-driven insights, compliance automation, and predictive analytics. For Malaysian banks and financial institutions, the appropriate platform to employ relies on size, regulator needs, and infrastructure maturity. With integrated robust security architecture and intelligent risk management instruments, XYZ Company has the potential to harden defenses, guard confidentiality, and resist disruption in the evolving digital space.

References

1. SecureTechIn. (2024). *Uncovering the possible Snowflake data breach of 2024: A deep dive into lessons and security strategy* [Video]. YouTube. https://www.youtube.com/watch?v=pqMLdKXbZ8U
2. Nair, P. (2024). *Salt Typhoon explained: Cyber espionage secrets* [Video]. YouTube. https://www.youtube.com/watch?v=MLdtDvzCiOQ

 doi:10.20944/preprints202504.2532.v1

3. YouTube. (2025). *Untitled video on IoT cyberattacks*. https://youtu.be/MYXIw5aqYNQ?si=qGLCpZ1_0kj0-T0T
4. Klingner, B. (2021). North Korean cyberattacks: A dangerous and evolving threat. *The Heritage Foundation*. https://www.heritage.org/asia/report/north-korean-cyberattacks-dangerous-and-evolving-threat
5. Kim, M.-H. (2022). North Korea's cyber capabilities and their implications for international security. *Sustainability*, *14*(3), 1744. https://doi.org/10.3390/su14031744
6. Derbyshire, R., Green, B., Prince, D., Mauthe, A., & Hutchison, D. (2018). An analysis of cybersecurity attack taxonomies. *IEEE Xplore*. https://doi.org/10.1109/EuroSPW.2018.00028
7. Kazi, N. F. (2024). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *ResearchGate*. https://www.researchgate.net/publication/378745228
8. Montini, H. (2024). *Snowflake breach: Everything we know so far*. ProvenData. https://www.provendata.com/blog/snowflake-data-breach/
9. Greenberg, A. (2025, February 13). China's Salt Typhoon spies are still hacking telecoms—Now by exploiting Cisco routers. *WIRED*. https://www.wired.com/story/chinas-salt-typhoon-spies-are-still-hacking-telecoms-now-by-exploiting-cisco-routers/
10. Forum of Incident Response and Security Teams (FIRST). (n.d.). *FIRST supported sustainable development goals (SDG)*. https://www.first.org/about/sdg
11. GeeksforGeeks. (2019). *Cyber crime*. https://www.geeksforgeeks.org/cyber-crime/
12. Cobb, M. (2022). *6 common types of cyber attacks and how to prevent them*. TechTarget. https://www.techtarget.com/searchsecurity/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them
13. Deloitte. (2022). *AI in financial services: Challenges and opportunities*. Deloitte Insights.
14. Bank Negara Malaysia. (2023). *Regulatory framework for financial institutions*. https://www.bnm.gov.my/legislation-guidelines
15. HSBC. (2022). *Automating compliance with IBM Watson*. https://www.hsbc.com
16. IBM. (n.d.). *IBM Watson for risk & compliance*. https://www.ibm.com
17. IBM. (2023a). *AI in financial services: Transforming risk management*. https://www.ibm.com
18. IBM. (2023b). *IBM Watson features for risk management*. https://www.ibm.com
19. IBM. (2023c). *Challenges in implementing AI for risk management*. https://www.ibm.com
20. Standard Chartered Bank. (2023). *AI-driven compliance solutions*. https://www.sc.com
21. Forbes. (2023). *The future of AI in financial services*. https://www.forbes.com
22. Palantir Technologies. (n.d.). *Palantir Foundry for transaction monitoring*. https://www.palantir.com/assets/xrfr7uokpv1b/...
23. Launch Consulting. (n.d.). *The path to scalability: How Snowflake and Palantir Foundry enhance business potential*. https://www.launchconsulting.com/posts/the-path-to-scalability-how-snowflake-and-palantir-foundry-enhance-business-potential
24. PeerSpot. (2014). *Pros and cons of Palantir Foundry 2025*. https://www.peerspot.com/products/palantir-foundry-pros-and-cons
25. Writer, S. (2025). *A comprehensive guide to understanding Palantir's technology and applications*. Reference.com. https://www.reference.com/world-view/comprehensive-guide-understanding-palantir-s-technology-applications
26. Malaysia Financial Sector Blueprint. (2022). *Future of finance in Malaysia: Digitalization and compliance*. Malaysian Government.
27. Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *ScienceDirect*, *4*, 186–202. https://www.sciencedirect.com/science/article/pii/S2667345223000561
28. BNM – Bank Negara Malaysia. (2023). *Regulatory framework for financial institutions*. https://www.bnm.gov.my/legislation-guidelines
29. Deloitte. (2022). *AI in financial services: Challenges and opportunities*. Deloitte Insights.
30. Derbyshire, R., Green, B., Prince, D., Mauthe, A., & Hutchison, D. (2018). An analysis of cybersecurity attack taxonomies. *IEEE Xplore*. https://doi.org/10.1109/EuroSPW.2018.00028

 doi:10.20944/preprints202504.2532.v1

31. Greenberg, A. (2025, February 13). China's Salt Typhoon spies are still hacking telecoms—Now by exploiting Cisco routers. *WIRED*. https://www.wired.com/story/chinas-salt-typhoon-spies-are-still-hacking-telecoms-now-by-exploiting-cisco-routers/
32. IBM. (2023b). *IBM Watson features for risk management*. https://www.ibm.com
33. IBM. (2023c). *Challenges in implementing AI for risk management*. https://www.ibm.com
34. Insight7. (2022). *Customer insights platform*. https://insight7.io/
35. Kim, M.-H. (2022). North Korea's cyber capabilities and their implications for international security. *Sustainability*, *14*(3), 1744. https://doi.org/10.3390/su14031744
36. Klingner, B. (2021). North Korean cyberattacks: A dangerous and evolving threat. *The Heritage Foundation*. https://www.heritage.org/asia/report/north-korean-cyberattacks-dangerous-and-evolving-threat
37. Malaysia Financial Sector Blueprint. (2022). *Future of finance in Malaysia: Digitalization and compliance*. Malaysian Government. https://www.bnm.gov.my/documents/20124/5915429/fsb3_en_book.pdf
38. Montini, H. (2024). *Snowflake breach: Everything we know so far*. ProvenData. https://www.provendata.com/blog/snowflake-data-breach/
39. Palantir Technologies. (n.d.). *Palantir Foundry for transaction monitoring*. https://www.palantir.com
40. Standard Chartered Bank. (2023). *AI-driven compliance solutions*. https://www.sc.com
41. Writer, S. (2025). *A comprehensive guide to understanding Palantir's technology and applications*. Reference.com. https://www.reference.com/world-view/comprehensive-guide-understanding-palantir-s-technology-applications.
42. Dogra, V., Singh, A., Verma, S., Kavita, Jhanjhi, N. Z., & Talib, M. N. (2021). Analyzing DistilBERT for sentiment classification of banking financial news. In S. L. Peng, S. Y. Hsieh, S. Gopalakrishnan, & B. Duraisamy (Eds.), *Intelligent computing and innovation on data science* (Vol. 248, pp. 665–675). Springer. https://doi.org/10.1007/978-981-16-3153-5_53
43. Gopi, R., Sathiyamoorthi, V., Selvakumar, S., et al. (2022). Enhanced method of ANN based model for detection of DDoS attacks on multimedia Internet of Things. *Multimedia Tools and Applications*, *81*(36), 26739–26757. https://doi.org/10.1007/s11042-021-10640-6
44. Chesti, I. A., Humayun, M., Sama, N. U., & Jhanjhi, N. Z. (2020, October). Evolution, mitigation, and prevention of ransomware. In *2020 2nd International Conference on Computer and Information Sciences (ICCIS)* (pp. 1–6). IEEE.
45. Alkinani, M. H., Almazroi, A. A., Jhanjhi, N. Z., & Khan, N. A. (2021). 5G and IoT based reporting and accident detection (RAD) system to deliver first aid box using unmanned aerial vehicle. *Sensors*, *21*(20), 6905.
46. Babbar, H., Rani, S., Masud, M., Verma, S., Anand, D., & Jhanjhi, N. (2021). Load balancing algorithm for migrating switches in software-defined vehicular networks. *Computational Materials and Continua*, *67*(1), 1301–1316.
47. Ashfaq, F., Jhanjhi, N. Z., Khan, N. A., Muzafar, S., & Das, S. R. (2024, March). CrimeScene2Graph: Generating Scene Graphs from Crime Scene Descriptions Using BERT NER. In *International Conference on Computational Intelligence in Pattern Recognition* (pp. 183-201). Singapore: Springer Nature Singapore.
48. Faisal, A., Jhanjhi, N. Z., Ray, S. K., Gururaj, H. L., Ashfaq, F., & Das, S. R. Splitfed learning methods for natural language processing.
49. Das, S. R., Jhanjhi, N. Z., Asirvatham, D., Ashfaq, F., Javed, D., & Gururaj, H. L. Blockchain-driven splitfed learning for data protection in IoT setting.
50. Ashfaq, F., Jhanjhi, N. Z., Khan, N. A., Ray, S. K., Gururaj, H. L., Faisal, A., & Das, S. R. Enhancing computational performance in healthcare through federated learning approach.
51. Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Lau, S. P., Muniandy, L., Gharib, A. H., ... & Murugesan, R. K. (2024). Industry 4.0: Future Trends and Research Directions. *Convergence of Industry 4.0 and Supply Chain Sustainability*, 342-405.
52. Kumar, A., Kumar, M., Verma, S., Kavita, Jhanjhi, N. Z., & Ghoniem, R. M. (2022). Vbswp-CeaH: vigorous buyer-seller watermarking protocol without trusted certificate authority for copyright Protection in cloud environment through additive homomorphism. *Symmetry*, *14*(11), 2441.

 doi:10.20944/preprints202504.2532.v1

53. Javed, D., Jhanjhi, N. Z., Khan, N. A., Ray, S. K., Al Mazroa, A., Ashfaq, F., & Das, S. R. (2024). Towards the future of bot detection: A comprehensive taxonomical review and challenges on Twitter/X. *Computer Networks*, *254*, 110808.
54. Das, S. R., Jhanjhi, N. Z., Asirvatham, D., Ashfaq, F., & Abdulhussain, Z. N. (2023, February). Proposing a model to enhance the IoMT-based EHR storage system security. In *International Conference on Mathematical Modeling and Computational Science* (pp. 503-512). Singapore: Springer Nature Singapore.
55. Faisal, A., Jhanjhi, N. Z., Ashraf, H., Ray, S. K., & Ashfaq, F. (2025). A Comprehensive Review of Machine Learning Models: Principles, Applications, and Optimal Model Selection. *Authorea Preprints*.
56. Alshudukhi, K. S., Ashfaq, F., Jhanjhi, N., & Humayun, M. (2024). Blockchain-Enabled Federated Learning for Longitudinal Emergency Care. *IEEE Access*.
57. Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, *22*(1), 105-117.
58. Javed, D., Jhanjhi, N. Z., & Khan, N. A. (2023, July). Explainable Twitter bot detection model for limited features. In *IET Conference Proceedings CP837* (Vol. 2023, No. 11, pp. 476-481). Stevenage, UK: The Institution of Engineering and Technology.
59. Srinivasan, K., Garg, L., Chen, B. Y., Alaboudi, A. A., Jhanjhi, N. Z., Chang, C. T., ... & Deepa, N. (2021). Expert System for Stable Pow