



☐ **Summative Feedback:**

☐ **Resubmission Feedback:**

**Grade:**

**Assessor Signature:**

**Date:**

**Internal Verifier's Comments:**

**Signature & Date:**

## Table of Contents

<b>A. INTRODUCTION.</b>	5
<b>B. Produce a research proposal that clearly defines a research question or hypothesis supported by a literature review (P1).</b>	5
1. Research Topic.	5
2. Abstracts.	5
3. Situation.	5
4. Define the main aims and objectives of the topic (Risks in computer system security and network security in Big Data Environments along with solutions to build better security systems)	7
5. Plan The Project.	8
<b>C. Examine appropriate research methods and approaches to primary and secondary research (P2).</b>	9
1. Research Method (Primary Research).	9
1.1. Primary Research?	9
1.2. Types of primary research.	10
1.3. Advantages and disadvantages of Primary Research.	11
2. Research Method (Secondary Research).	12
2.1. Secondary Research?	12
2.2. Types of secondary research.	13
2.3. Advantages and disadvantages of Secondary Research.	14
3. Qualitative research method.	15
3.1. Characteristics of Qualitative Research.	15
3.2. Advantages and disadvantages of qualitative research method.	16
4. Quantitative research method.	17
4.1. Characteristics of Quantitative Research.	18
4.2. Advantages and disadvantages of quantitative research method.	19
<b>D. Conduct primary and secondary research using appropriate methods for a computing research project that consider costs, access and ethical issues (P3).</b>	20
1. Do Secondary Research.	20
1.1. Sources.	21
1.2. Interpretation and implications of the findings.	24
2. Do Primary Research.	25
2.1. Overall research design.	25
2.2. Interview.	26
2.3. Survey	28

<b>E. Apply appropriate analytical tools, analyse research findings and data (P4).....</b>	<b>30</b>
1. Interview Results. ....	30
1.1. Interview 1.....	30
1.2. Interview 2.....	33
1.3. Interview 3.....	35
1.4. Interview 4.....	38
1.5. Interview 5.....	41
1.6. Interview Summary:.....	44
2. Survey Results.....	46
3. Analyze the results of the primary research .....	57
<b>F. Communicate research outcomes in an appropriate manner for the intended audience (P5).....</b>	<b>58</b>
1. Conclusion .....	59
2. Recommendations .....	59
<b>G. Appendix. ....</b>	<b>60</b>
1. Research Proposal Form. ....	60
2. Ethical form. ....	66
<b>H. CONCLUSION. ....</b>	<b>69</b>
<b>I. REFERENCE.....</b>	<b>69</b>
Figure 1: WBS of the project.....	9
Figure 2: Primary Research Methods.....	10
Figure 3: Secondary Research Method. ....	13
Figure 4: Qualitative Research Method. ....	15
Figure 5: Quantitative Research Methods. ....	18
Figure 6: Survey 1.....	48
Figure 7: Survey 2.....	48
Figure 8: Survey 3.....	49
Figure 9: Survey 4.....	49
Figure 10: Survey 5.....	50
Figure 11: Survey 6. ....	50
Figure 12: Survey 7.....	51
Figure 13: Survey 8.....	51
Figure 14: Survey 9.....	52
Figure 15: Survey 10.....	52
Figure 16: Survey 11.....	53
Figure 17: Survey 12.....	54

Figure 18: Survey 13.....	54
Figure 19: Survey 14.....	55

## A. INTRODUCTION.

In the last decade, Big Data has seen an exponential surge, demanding advanced computational abilities to process vast and varied data. It's a vital asset for industries, enabling informed decisions and fostering innovation. However, this growth raises major security, ethical, and sustainability concerns, especially in computer and network security. This research focuses on exploring risks and proposed solutions at the intersection of Big Data and security, aiming to enhance data ecosystem security in this data-driven era. Realizing this problem, I will research and collect information with the topic "Risks in computer system security and network security in Big Data Environments along with solutions to build better security systems."

## B. Produce a research proposal that clearly defines a research question or hypothesis supported by a literature review (P1).

### 1. Research Topic.

"Risks in computer system security and network security in Big Data Environments along with solutions to build better security systems."

### 2. Abstracts.

In the era of rapid digital growth, Big Data environments face serious security risks. This research aims to investigate these risks and propose solutions. Big Data, rich in sensitive information, is a prime target for cyber threats like unauthorized access and data breaches. This study categorizes these risks and explores tools like encryption, access controls, and AI-based threat detection to enhance security. Simulations are used to test proposed security measures. Ultimately, this research aims to lay a strong foundation for proactive and resilient security systems in the age of Big Data.

### 3. Situation.

#### - Situation Overview:

The advent of Big Data has led to a revolution in how organizations manage, analyze, and utilize data. However, this surge in data usage and storage has placed immense pressure on

ensuring the security and integrity of this invaluable resource. Cyber threats, including unauthorized access, data breaches, malware attacks, and insider threats, pose significant risks to the confidentiality, availability, and integrity of data within these expansive systems. As a result, organizations grappling with Big Data must navigate a complex security landscape to safeguard their digital assets and maintain the trust of their stakeholders.

- **Risks Identified:**

- **Unauthorized Access and Data Breaches:** Unauthorized access to sensitive data repositories and subsequent data breaches can lead to severe financial and reputational losses.
- **Malware Attacks:** Malicious software infiltrating the system can cause disruptions, compromise data integrity, and allow unauthorized access.
- **Insider Threats:** Disgruntled employees or individuals with privileged access can intentionally or unintentionally compromise security measures.
- **Data Tampering and Manipulation:** Malevolent actors may alter or manipulate critical data, leading to inaccurate analyses and flawed decision-making.
- **Inadequate Encryption and Data Security:** Weak encryption protocols and lax data security measures can expose sensitive information, making it susceptible to unauthorized access and theft.

- **Solutions Proposed:**

- **Advanced Encryption and Authentication Mechanisms:** Implementing robust encryption algorithms and multifactor authentication systems to ensure data security and limit unauthorized access.
- **Regular Security Audits and Vulnerability Assessments:** Conducting periodic security audits and vulnerability assessments to identify weaknesses and proactively address potential threats.
- **Employee Training and Awareness:** Conducting regular training programs to educate employees about cybersecurity best practices and creating a security-conscious organizational culture.

- **Real-time Monitoring and Intrusion Detection Systems:** Utilizing real-time monitoring tools and intrusion detection systems to promptly detect and respond to security breaches and anomalies.
- **Data Integrity Checks and Validation:** Implementing robust data validation mechanisms to ensure the integrity and authenticity of the stored data.

#### 4. Define the main aims and objectives of the topic (Risks in computer system security and network security in Big Data Environments along with solutions to build better security systems)

The main aims and objectives of the topic "Risks in computer system security and network security in Big Data Environments along with solutions to build better security systems" are defined to comprehensively address the pressing concerns and challenges posed by the intersection of Big Data environments and cybersecurity. These aims and objectives guide the research and initiatives aimed at fortifying computer system security, network security, and data protection within the context of Big Data. They encompass understanding risks, proposing effective solutions, and promoting a proactive security posture to ensure the integrity and confidentiality of data.

##### - **Aims:**

- **Risk Assessment and Understanding:** To comprehensively identify, categorize, and understand the various risks associated with computer system security and network security within Big Data environments.
- **Environmental and Regulatory Compliance:** To ensure compliance with environmental regulations and ethical considerations while fortifying security measures, aiming for a sustainable and responsible approach.
- **Security Enhancement and Solutions:** To propose and implement advanced security solutions and practices that mitigate identified risks and vulnerabilities effectively.

##### - **Objectives:**

- **Risk Profiling and Analysis:** Conduct a thorough analysis of potential risks, including unauthorized access, data breaches, malware attacks, and insider threats specific to Big Data environments.

- **Vulnerability Identification and Assessment:** Identify vulnerabilities in computer systems, network infrastructure, and data storage models and assess their potential impact on security.
- **Security Measures Tailored to Big Data:** Develop security measures specifically tailored to Big Data environments, considering the unique characteristics and challenges associated with large-scale data storage and processing.
- **Data Encryption and Privacy:** Implement advanced encryption techniques to ensure data privacy and protect sensitive information from unauthorized access or interception during transmission and storage.
- **Access Control and Authentication Enhancements:** Enhance access control mechanisms and authentication processes to minimize unauthorized access and fortify security within the network.
- **Employee Training and Security Awareness:** Conduct regular training programs to educate employees about cybersecurity best practices, ensuring they are well-equipped to contribute to a security-conscious organizational culture.

## 5. Plan The Project.

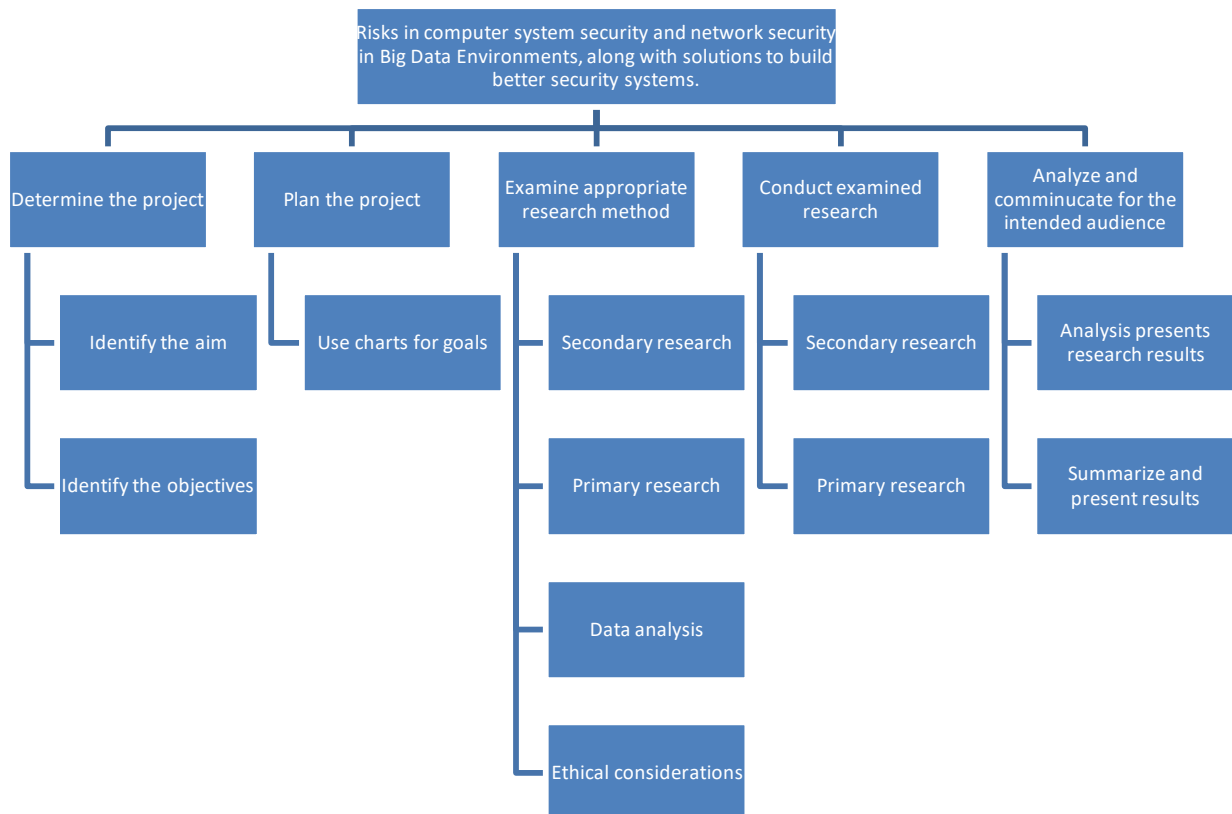
In outlining the project plan, it is paramount to delineate a structured approach encompassing essential phases for its successful execution. The comprehensive project plan will encompass several vital components that need to be meticulously considered and articulated, starting with a clear delineation of the project's objectives, goals, and overall purpose.

- **Defining the Project's Scope and Objectives:** The foundational step involves a thorough definition of the project's scope, objectives, and ultimate goal. This includes precisely outlining what is to be achieved, the problem to be addressed, or the opportunity to be leveraged through the project.
- **Research Methodology Selection:** Choosing the appropriate research methodology is a pivotal decision. This step entails an in-depth exploration of various research methods, weighing the merits and demerits of primary research, secondary research, or a



combination of both, to ascertain the most suitable approach for gathering data and insights.

- **Conducting Preliminary Research:** Prior to delving into the project, a preliminary research phase is imperative. This involves an extensive literature review, market analysis, or any background research necessary to understand the context, identify gaps in existing knowledge, and establish a solid foundation for the subsequent phases of the project.



*Figure 1: WBS of the project.*

## C. Examine appropriate research methods and approaches to primary and secondary research (P2).

### 1. Research Method (Primary Research).

#### 1.1. Primary Research?

Primary research involves gathering firsthand information directly from the source. In the context of the topic "Risks in computer system security and network security in Big Data Environments along with solutions to build better security systems," conducting primary research involves collecting new and original data directly related to the subject

matter. This data is collected through various methodologies and techniques to address specific research objectives.



*Figure 2: Primary Research Methods.*

## 1.2. Types of primary research.

Primary research involves collecting original data directly from the source to address a specific research question or objective. There are various types of primary research methods, each with its own advantages and suitability depending on the research goals, resources, and target audience. Here are the main types of primary research:

- **Surveys:** Surveys involve structured questionnaires or interviews distributed to a targeted sample to collect data on opinions, attitudes, behaviors, or demographics. Surveys can be conducted through face-to-face interviews, phone calls, email, or online platforms.
- **Interviews:** Interviews are in-depth conversations between a researcher and a participant or a group of participants. Interviews can be structured, semi-structured, or unstructured, allowing for a detailed exploration of a topic or issue.
- **Focus Groups:** Focus groups involve a small group of participants (6-12) discussing a specific topic under the guidance of a facilitator. This method encourages

interaction and allows for the exploration of diverse perspectives within a group setting.

- **Observational Research:** Observational research involves direct observation of individuals, behaviors, and events in natural settings. Researchers record observations to understand behaviors, interactions, and phenomena without intervening.
- **Experiments:** Experiments are controlled studies where researchers manipulate variables to observe the effects and relationships between them. Experiments allow for causal inferences and controlled testing of hypotheses.

### 1.3. Advantages and disadvantages of Primary Research.

Primary Research	
Advantages	Disadvantages
<b>Originality and Freshness of Data:</b> Primary research provides new and firsthand information specifically tailored to the research objectives, ensuring the data is relevant, up-to-date, and unique.	<b>Resource-Intensive:</b> Primary research can be time-consuming, labor-intensive, and costly, especially when considering participant recruitment, data collection, and analysis.
<b>Specific to Research Objectives:</b> Researchers can design primary research to precisely address their research questions, enabling targeted and focused data collection that aligns with the study's goals.	<b>Limited Scale and Scope:</b> Due to resource constraints, primary research may involve a smaller sample size or cover a limited geographic area, potentially limiting the generalizability of findings.
<b>Control over Data Collection:</b> Researchers have control over the research design, data collection methods, and the quality of data, allowing for customized approaches to meet the study's requirements.	<b>Data Collection Challenges:</b> Conducting interviews, surveys, or experiments may face challenges such as non-response, participant hesitancy, or difficulties in accurately measuring certain variables.

<b>Customization and Flexibility:</b> Primary research methods can be customized and adapted to the research context, making it flexible and suitable for a wide range of research topics and objectives.	<b>Ethical Considerations:</b> Ethical concerns related to participant privacy, informed consent, and potential harm may arise, necessitating careful planning and adherence to ethical guidelines.
<b>In-Depth Understanding:</b> Primary research methods like interviews, focus groups, and observations facilitate a deeper understanding of attitudes, behaviors, and motivations by allowing direct interaction with participants.	<b>Time Constraints:</b> Primary research often requires substantial time to plan, conduct, and analyze, which may not always align with project timelines or deadlines.
<b>Causal Relationships:</b> Through experiments and controlled conditions, primary research can establish cause-and-effect relationships between variables, enhancing the understanding of phenomena.	<b>Complexity of Analysis:</b> Analyzing primary data may require specialized knowledge or expertise, particularly when dealing with complex statistical methods or intricate qualitative analysis.

## 2. Research Method (Secondary Research).

### 2.1. Secondary Research?

Secondary research, also known as desk research, involves the use of existing data, information, and published sources to gather insights, analyze trends, or support research objectives without directly collecting new data from primary sources. It entails reviewing and synthesizing materials that have already been created by other researchers, institutions, organizations, or publications. These existing sources serve as the basis for analysis, evaluation, and building an understanding of a specific topic, issue, or research question.



**Figure 3: Secondary Research Method.**

## 2.2. Types of secondary research.

Secondary research is a research method that involves using already existing data. Existing data is summarized and collated to increase the overall effectiveness of the research. One of the key advantages of secondary research is that it allows us to gain insights and draw conclusions without having to collect new data ourselves. This can save time and resources and also allow us to build upon existing knowledge and expertise. When conducting secondary research, it's important to be thorough and thoughtful in our approach. This means carefully selecting the sources and ensuring that the data we're analyzing is reliable and relevant to the research question. It also means being critical and analytical in the analysis and recognizing any potential biases or limitations in the data.

- **Data Sources:** Secondary research sources include academic journals, books, government publications, reports, magazines, newspapers, online articles, white papers, conference proceedings, theses, dissertations, and websites.
- **Nature of Data:** Data obtained from secondary sources is pre-existing and has already been analyzed or interpreted by the original authors or sources. It is essentially a compilation of previously collected data.
- **Objective:** The primary objective of secondary research is to gather, synthesize, and analyze information to inform or support the research, validate findings, or generate new insights without directly collecting data from primary sources.

- **Method of Collection:** Researchers gather secondary data from publicly available sources or through subscriptions to academic databases, libraries, online repositories, and other accessible platforms.
- **Data Analysis:** Analysis in secondary research involves interpreting, evaluating, comparing, contrasting, and synthesizing the existing data from various sources to draw conclusions or identify patterns, trends, and gaps in knowledge.

### 2.3. Advantages and disadvantages of Secondary Research.

Secondary Research	
Advantages	Disadvantages
<b>Time and Cost-Effective:</b> Secondary research saves time and resources as data is readily available from existing sources, eliminating the need for data collection.	<b>Limited Control over Data Quality:</b> Researchers have limited control over the quality, accuracy, and completeness of the data obtained from secondary sources.
<b>Wide Range of Sources:</b> Researchers can access a vast array of sources, including academic papers, books, reports, government publications, articles, and online databases.	<b>Potential Bias in Source Selection:</b> Bias may be introduced based on the selection of sources, leading to a skewed representation of the topic.
<b>Historical Data Analysis:</b> Researchers can analyze historical data to identify trends, patterns, and changes over time, providing valuable insights into the topic.	<b>Outdated Information:</b> The data retrieved may be outdated, especially in rapidly evolving fields, impacting the relevance and applicability of the findings.
<b>Comparative Analysis:</b> Multiple studies and sources allow for comparative analysis, helping researchers assess consistencies, discrepancies, or changes in findings.	<b>Lack of Specificity:</b> Secondary data may not align precisely with the research objectives, necessitating compromises in terms of specificity and relevance.
<b>Large Sample Sizes:</b> Secondary research often involves extensive sample sizes or datasets,	<b>Limited Contextual Understanding:</b> Existing data may lack the contextual understanding of

enabling researchers to analyze data at a larger scale.	the research setting or may not cover certain dimensions of the topic in detail.
<b>Non-Intrusive:</b> Secondary research is non-intrusive and does not involve direct interaction with individuals, ensuring privacy and ethical considerations.	<b>Potential Plagiarism Concerns:</b> Proper citation and avoidance of plagiarism are crucial when using existing information, requiring researchers to give appropriate credit to original authors.

### 3. Qualitative research method.

Qualitative research is a research method that focuses on understanding and interpreting human behavior, experiences, perspectives, and social phenomena. It emphasizes the exploration of subjective aspects, allowing researchers to delve into the depth and complexity of a particular topic. Qualitative research methods are particularly valuable for gaining insights into motivations, opinions, beliefs, and cultural contexts.



*Figure 4: Qualitative Research Method.*

#### 3.1. Characteristics of Qualitative Research.

- **Non-numeric:** Qualitative research typically involves non-numeric data that cannot be measured or quantified. Researchers use words, images, and other forms of non-numeric data to understand and interpret phenomena.
- **Emergent design:** Qualitative research often involves an emergent design, which means that the research design evolves as the study progresses. Researchers may modify the research questions or methods as they learn more about the research subject.
- **Inductive:** Qualitative research typically involves an inductive approach, which means that theories and hypotheses are developed from the data rather than being imposed on the data beforehand.
- **Contextual:** Qualitative research takes into account the context in which the data is collected. The researcher aims to understand the meaning of the data in its particular setting and considers how social, cultural, and historical factors may impact the research.
- **Subjectivity:** Qualitative research acknowledges the role of the researcher in the research process. The researcher's interpretations, biases, and values are taken into consideration when analyzing the data. This subjectivity is seen as a strength rather than a weakness, as it allows for a more nuanced and in-depth understanding of the research topic.
- **Nonlinear:** The process of qualitative research is often nonlinear and iterative, with data collection, analysis, and interpretation occurring simultaneously. The researcher may revisit and revise their research questions and methods as new insights emerge from the data.

### 3.2. Advantages and disadvantages of qualitative research method.

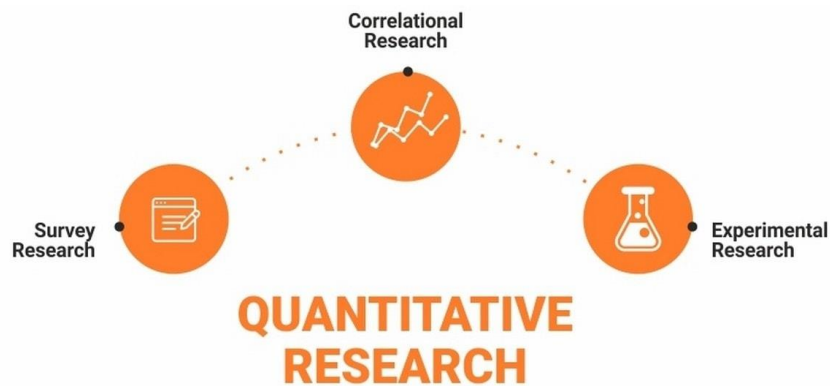
Qualitative Research Method	
Advantages	Disadvantages
<b>Rich and In-Depth Insights:</b> Qualitative research provides detailed and	<b>Subjectivity and Bias:</b> Qualitative research is susceptible to researcher bias and



comprehensive insights into complex social phenomena, allowing for a deep understanding of behaviors, attitudes, and motivations.	subjectivity, as the researcher's interpretation and analysis may be influenced by personal beliefs, values, and experiences.
<b>Flexibility and Adaptability:</b> Qualitative research methods can be adapted and adjusted during the study to explore unexpected themes or emerging patterns, enhancing flexibility in data collection and analysis.	<b>Time and Resource Intensive:</b> Qualitative research can be time-consuming and resource-intensive due to data collection methods such as interviews, transcription, and detailed analysis required for rich insights.
<b>Contextual Understanding:</b> Qualitative research emphasizes understanding behavior within its natural context, capturing the holistic picture and enabling researchers to explore the social and cultural influences on the topic.	<b>Small Sample Sizes:</b> Due to the in-depth nature of qualitative research, sample sizes are often small, limiting the generalizability of findings to a broader population.
<b>Exploratory and Hypothesis Generation:</b> Qualitative research is often exploratory and helps generate hypotheses and theories that can be further tested using quantitative methods.	<b>Difficulty in Standardization:</b> Standardization and replicability can be challenging in qualitative research due to the personalized and context-specific nature of the data collected.
<b>Participant Perspectives:</b> Qualitative research values the perspectives, opinions, and experiences of participants, giving voice to their narratives and allowing researchers to capture diverse viewpoints.	<b>Data Interpretation Complexity:</b> Analyzing qualitative data can be complex, requiring advanced skills and expertise to interpret themes, patterns, and meanings accurately.

#### 4. Quantitative research method.

Quantitative research is a research method that involves the systematic collection, analysis, interpretation, and presentation of numerical data to understand, describe, or predict phenomena of interest. This approach emphasizes objective measurements, statistical analysis, and the use of structured research instruments such as surveys, questionnaires, and experiments. Quantitative research aims to identify patterns, relationships, and cause-and-effect interactions within a population or sample.



*Figure 5: Quantitative Research Methods.*

#### 4.1. Characteristics of Quantitative Research.

Quantitative research is characterized by specific features and attributes that distinguish it from other research methods. Here are the key characteristics of quantitative research:

- **Objective and Empirical:** Quantitative research is based on observable, measurable phenomena. It focuses on gathering data that can be analyzed statistically to draw objective conclusions and make empirical generalizations.
- **Numerical Data Collection:** Quantitative research involves the collection of numerical data through structured research instruments, such as surveys, questionnaires, and experiments. The data is typically quantifiable and represented in numerical form.
- **Structured Research Instruments:** Researchers use standardized and structured research instruments to gather data, including closed-ended questions with

predefined response options. This allows for consistent data collection and comparisons.

- **Statistical Analysis:** Quantitative research employs statistical analysis techniques to process and interpret data. This includes various statistical tests, measures of central tendency, dispersion, correlation, regression, and hypothesis testing.
- **Large Sample Sizes:** Quantitative research often requires a large and representative sample size to ensure statistical validity and generalizability of findings to a broader population.

#### 4.2. Advantages and disadvantages of quantitative research method.

Quantitative Research Method	
Advantages	Disadvantages
<b>Objectivity and Reliability:</b> Quantitative research maintains a high degree of objectivity through standardized data collection methods and statistical analysis, resulting in reliable and consistent findings.	<b>Lack of Contextual Understanding:</b> Quantitative research often overlooks the depth of understanding provided by the context, as it focuses primarily on numerical data and may miss the underlying reasons or motivations.
<b>Large Sample Sizes:</b> Quantitative research often involves large sample sizes, enhancing the generalizability and external validity of the research outcomes to a broader population.	<b>Simplification of Complex Phenomena:</b> Quantitative research tends to oversimplify complex phenomena by breaking them down into measurable variables, potentially losing the richness and intricacies of the subject.
<b>Statistical Analysis:</b> Quantitative research employs statistical techniques to analyze data, allowing for the identification of patterns, trends, and relationships between variables in a systematic and precise manner.	<b>Limited Exploration of New Insights:</b> The rigid structure of quantitative research may limit the exploration of unexpected insights or phenomena that were not initially considered in the study design.

<b>Numerical Data:</b> Quantitative research generates numerical data that can be quantified, compared, and statistically tested, providing a clear basis for drawing conclusions and making predictions.	<b>Inadequate for Sensitive Topics:</b> Quantitative research may not be suitable for studying sensitive or deeply personal topics, as the fixed response options may not capture the complexity of individuals' experiences.
---	---

#### **D. Conduct primary and secondary research using appropriate methods for a computing research project that consider costs, access and ethical issues (P3).**

In this research, we're using a blend of primary and secondary research methods to study computer and network security risks in Big Data Environments. We're focusing on collecting detailed data to thoroughly understand the research problem. Our approach combines quantitative and qualitative research for a well-rounded perspective. Quantitative research provides structured and objective data, ideal for rigorous analysis, while qualitative research offers valuable subjective insights. By integrating both, we aim to achieve accurate and comprehensive research findings, aligning with our commitment to ethical and effective security enhancement in Big Data Environments.

##### **1. Do Secondary Research.**

To deepen my understanding of the risks in computer system security and network security in Big Data Environments, as well as the search for solutions to build better security systems, I undertook a comprehensive secondary research effort. This research was conducted with the aim of collecting and synthesizing existing information from a wide array of authoritative and relevant academic sources, which encompassed journals, industry reports, official government statistics, and reputable news articles.

- **Publication Date:** Preference was given to recent sources, as they offer insights into the most up-to-date developments and trends in computer system and network security within Big Data Environments. However, historical perspectives were also considered if they provided valuable contextual information.

- **Source Reputation:** Sources from reputable publications, organizations, and academic institutions were prioritized to ensure that the information gathered came from trusted and credible outlets.
- **Author Expertise:** The qualifications, expertise, and credentials of the authors were evaluated. Information provided by experts in the field was deemed more reliable.
- **Relevance to the Research Topic:** Each source was assessed for its direct relevance to the research topic of risks in computer system security and network security in Big Data Environments. Irrelevant or tangential sources were excluded.

By adhering to these rigorous selection criteria, I aimed to compile a well-rounded and trusted body of information to serve as a solid foundation for research on this critical topic. The diverse range of sources and their collective expertise provided a comprehensive view of the subject, enabling a thorough analysis of the risks and potential solutions concerning computer system and network security within Big Data Environments.

### 1.1. Sources.

- What is Big Data Security? Challenges & Solutions

**Link:** Crockett, E. (2023) What is Big Data Security? Challenges & Solutions, Datamation.

Available at: <https://www.datamation.com/big-data/big-data-security/> (Accessed: 6 October 2023).

**Data collected:** The data collected from the provided text highlights the critical aspects of big data security, including the challenges, benefits, technologies, and the role of various stakeholders. Here's a summarized version: The text underscores the importance of big data security, aimed at securing a company's valuable business data for ongoing safe and compliant operations. It highlights the vulnerabilities Big Data deployments face, making them attractive targets for potential invaders, posing risks such as data unauthorized access, and ransomware attacks. Securing big data platforms requires a combination of traditional security tools, innovative toolsets, and intelligent monitoring processes throughout the platform's life cycle. The discussion delves into how big data security operates, emphasizing the need to secure data at various stages: data sources, stored

data, and output data. The data sources are diverse, ranging from user-generated data to machine-generated data, emphasizing the need to secure data in transit from these sources. The stored data requires mature security toolsets, including encryption at rest and strong user authentication. Output data, which is the outcome of extensive analytics, is considered valuable and must be encrypted and compliant with regulations. The text outlines the benefits of big data security, including customer retention, risk identification, business innovation, and cost optimization. However, it also points out the challenges such as vulnerabilities of newer technologies, variable impact, unauthorized access, scale-related audit issues, and the need for constant updates. Key big data security technologies are discussed, including encryption, centralized key management, user access control, intrusion detection and prevention, and physical security. The importance of effective implementation and regular security monitoring is emphasized, including training for internal users and adherence to security best practices. Finally, the responsibility for big data security is highlighted as a collective effort involving IT, database administrators, compliance officers, business units, and end-users. The text highlights by highlighting big data security companies like Snowflake, Teradata, Cloudera, IBM, and Oracle, focusing on their contributions to the field. In summary, the collected data underscores the significance of big data security, detailing its operations, benefits, challenges, technologies, implementation strategies, and the collective responsibility involved in ensuring the security of valuable data in the realm of Big Data.

- Types of Computer Security Threats and How to Avoid Them

**Link:** Types of Computer Security Threats and (no date) Webroot. Available at:

<https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats>

(Accessed: 6 October 2023).

**Data collected:** The provided data includes a comprehensive exploration of cybersecurity threats prevalent in the online landscape. Cyber threats continually evolve and showcase their innovative nature, making it imperative to remain informed and vigilant. Key threats discussed in this data include computer viruses, spyware, hackers, predators, and phishing attempts. In understanding computer viruses, they are defined as harmful programs that

alter a computer's operations without the user's consent, replicating and causing damage during the process. Mitigating this threat necessitates cautious downloading practices and keeping antivirus software up to date. Spyware, another significant threat, monitors online activities or installs programs without consent, capturing personal information and invading privacy. Vigilance, reading terms and conditions, and being cautious of unknown advertisements are vital measures in combating spyware. The mention of hackers and predators underscores the human element in creating security threats. These exploit computer systems for personal gain or cyber-terrorism, compromising sensitive data, stealing identities, and gaining individuals unauthorized access. Effective protection involves leveraging online security tools and identity theft prevention mechanisms. Phishing, a prevalent threat, involves cybercriminals masquerading as trusted entities to deceive users into revealing sensitive information. Recognizing phishing scams and utilizing antivirus solutions with identity theft protection are effective strategies in preventing phishing attacks. Overall, staying informed about these threats and leveraging proactive security measures is crucial in maintaining online safety.

- Data Security

**Link:** What is Data Security: Threats, Risks & Solutions: Imperva (2023) Learning Center.

Available at: <https://www.imperva.com/learn/data-security/data-security/> (Accessed: 6 October 2023).

**Data collected:** Data security entails safeguarding corporate data to prevent unauthorized access and data loss. It encompasses protection against a range of cyber threats, including ransomware, data modification, and unauthorized access. Compliance with data protection regulations is crucial for industries processing sensitive information, such as payment card data or private health information in healthcare. Beyond compliance, data security is vital for modern businesses, directly impacting assets and customer data, with the average cost of data breaches being substantial. Social engineering, ransomware, and advanced persistent threats have emerged as significant threats in recent years. Effective data security necessitates a combination of techniques like data discovery, classification, data masking, and penetration testing. In addition, securing data in the cloud, database

security, big data security, and securing data in enterprise applications are essential aspects of an organization's overall data security strategy, each demanding a tailored approach. Regular review and adaptation of security measures remain crucial to ensure robust protection against evolving cyber threats.

## **1.2. Interpretation and implications of the findings.**

The comprehensive secondary research conducted on risks in computer system security and network security in Big Data Environments, along with solutions to enhance security systems, revealed significant insights and implications for the field. The interpretation of the findings sheds light on the urgency of addressing security concerns in the ever-evolving landscape of Big Data.

- **Heightened Awareness of Security Risks:** The research highlighted an increasing awareness of the diverse range of security risks associated with computer system and network security in Big Data Environments. Data breaches, cyber-attacks, insider threats, and scalability challenges emerged as major concerns. This heightened awareness emphasizes the need for proactive measures to mitigate these risks effectively.
- **Need for Evolved Security Measures:** The evolving landscape of technology necessitates security measures that continuously adapt and strengthen. The findings underscore the need for evolved security protocols, such as enhanced encryption, multi-factor authentication, and advanced behavioral analysis. These measures are critical for countering sophisticated cyber threats that exploit vulnerabilities in complex Big Data systems.
- **Importance of Access Control and Monitoring:** The research emphasized the significance of robust access control policies and monitoring mechanisms. Restricting access to sensitive data and closely monitoring system activities help mitigate insider threats and unauthorized access. Effective access control, combined with real-time monitoring, is crucial in maintaining the integrity and confidentiality of data.
- **Integration of Behavioral Analysis:** The inclusion of behavioral analysis and anomaly detection emerged as a promising approach. By leveraging advanced analytics, organizations can detect unusual patterns of behavior within the system, enabling early



identification of potential security threats. This proactive approach enhances the overall security posture and aids in swift response to potential breaches.

- **Continuous Security Audits and Updates:** The research highlighted the importance of regular security audits and timely updates. Security audits are vital to identifying vulnerabilities and ensuring compliance with security standards. Likewise, regularly updating systems and software with the latest security patches is essential in addressing emerging threats and minimizing security gaps.
- **Challenges and Opportunities for Innovation:** The study exposed challenges related to scalability and the constant evolution of cyber threats. However, it also presents opportunities for innovation and research. Innovations in encryption technologies, artificial intelligence for security, and collaboration among cybersecurity experts and organizations can help address these challenges effectively.
- **Strategic Decision-making for Organizations:** Organizations can leverage the research findings to make informed and strategic decisions regarding their security measures. By understanding the specific risks and suitable solutions for their Big Data environments, organizations can tailor their security strategies to align with their unique needs and risks.

In conclusion, the interpretation of the findings from the secondary research underscores the critical nature of addressing security concerns in Big Data Environments. It highlights the need for a multi-faceted approach that integrates advanced security measures, regular audits, and an agile response to emerging threats. Implementing these strategies will enable organizations to navigate the evolving cybersecurity landscape and protect their valuable data assets effectively.

## 2. Do Primary Research.

### 2.1. Overall research design

The research design for investigating risks in computer system security and network security in Big Data Environments, along with exploring solutions to enhance security systems, was meticulously structured to ensure a robust and comprehensive approach to data collection and analysis.

- **Expert Interviews:** Structured interviews were conducted with cybersecurity experts and professionals specializing in Big Data security. The purpose of these interviews was to gain

valuable insights, expert opinions, and practical experiences related to security risks and potential solutions. The interviewees were selected based on their expertise and experience in the field, ensuring diverse perspectives and depth of knowledge.

- **Survey:** A targeted survey was designed and distributed to a select group of professionals working in the field of cybersecurity and Big Data. The survey aimed to gather quantitative data on the perception of security risks, the effectiveness of current security measures, and the most pressing concerns within Big Data Environments. The survey questions were carefully crafted to obtain specific insights and feedback relevant to the research objectives.
- **Ethical Considerations:** Ethical considerations played a pivotal role in the research design to ensure the responsible conduct of research and the protection of participants' rights and privacy. The following ethical principles were adhered to throughout the research process:
  - **Informed Consent:** Participants in interviews and surveys were provided with clear information about the research objectives, their role, and the potential use of their data. Consent was obtained before proceeding with data collection.
  - **Anonymity and Confidentiality:** Participants' identities and responses were kept anonymous and confidential to encourage honest and uninhibited sharing of information. Data was stored securely and used only for the purpose of the research.
  - **Voluntary Participation:** Participation in interviews and surveys was entirely voluntary. Participants had the right to withdraw at any stage without any repercussions.

## 2.2. Interview

The interview process for this research is designed to gather expert insights and practical experiences pertaining to risks in computer system security and network security within Big Data Environments, as well as potential solutions to enhance security systems. The structured interview will be conducted with cybersecurity professionals and experts in the field. The questions are designed to encourage detailed responses and facilitate a comprehensive understanding of the subject.

### Questions:

- **Introduction and Background:** Could you please introduce yourself, highlighting your expertise and experience in the field of cybersecurity, particularly in the context of Big Data Environments?
- **Experience with Big Data Security:** Can you describe your experience dealing with security challenges specific to Big Data Environments? Are there any particular incidents or scenarios you've encountered that exemplify these challenges?
- **Identifying Key Security Risks:** What, in your opinion, are the most significant security risks in computer system and network security within Big Data Environments?
- **Data Privacy and Compliance:** How do you see data privacy and compliance concerns affecting security measures in Big Data? Are there specific compliance regulations that significantly impact security strategies?
- **Insider Threats:** How do insider threats manifest within Big Data Environments, and what measures do you recommend to mitigate these risks effectively?
- **Advanced Encryption Techniques:** What advancements in encryption techniques do you consider crucial for ensuring data security within Big Data Environments? How can organizations effectively implement these techniques?
- **Role of Machine Learning and AI:** How can machine learning and artificial intelligence be leveraged to bolster security measures in Big Data? Can you provide examples of successful implementations?
- **Access Control and Authorization:** How can robust access control policies and authorization mechanisms enhance security? What best practices would you recommend in this regard?
- **Understanding Firewalls in Big Data:** In the context of Big Data Environments, how would you define the role and significance of firewalls in ensuring cybersecurity?
- **Optimal Firewall Configurations for Big Data:** What firewall configurations and settings do you recommend for securing computer systems in Big Data Environments? Are there specific features or rules that should be prioritized?

- **Network Segmentation:** How can network segmentation be effectively employed in conjunction with firewalls to enhance security in Big Data Environments? Can you provide practical examples?
- **Adaptive and Next-Gen Firewalls:** What are the advantages of using adaptive and next-gen firewalls in Big Data Environments? Can you share examples of their successful implementation?
- **Recommendations for Optimizing Firewall Security in Big Data:** Based on your expertise, what recommendations would you provide to organizations aiming to optimize firewall security within Big Data Environments?
- **Closing Remarks:** Is there any additional insight, perspective, or recommendation you would like to share regarding the role of firewalls in securing computer systems within Big Data Environments?

### 2.3. Survey

The survey aims to gather insights and perceptions from professionals in the field of cybersecurity, specifically focusing on risks in computer system security and network security within Big Data Environments, along with potential solutions to enhance security systems. The survey is designed to elicit both qualitative and quantitative responses to better understand current practices, challenges, and emerging trends.

#### Questions:

- **Role and Experience:**
  - Please specify your role in the field of cybersecurity (e.g., security analyst, network engineer, cybersecurity manager).
  - How many years of experience do you have in the field of cybersecurity?
- **Industry and Organization:**
  - Which industry or sector does your organization primarily operate in?
  - What is the size of your organization (small, medium, large)?
- **Perceived Security Risks:**

- On a scale of 1 to 5, with 1 being the least significant and 5 being the most significant, please rate the perceived security risks in Big Data Environments (e.g., data breaches, insider threats, scalability challenges).
- **Major Concerns:**
  - What are your major concerns regarding security in Big Data Environments? Please provide a brief description.
- **Specific Security Challenges:**
  - In your opinion, what unique security challenges do Big Data Environments present compared to traditional data environments?
- **Effectiveness of Current Security Measures:**
  - On a scale of 1 to 5, how effective do you perceive the current security measures in place within Big Data Environments?
- **Key Security Measures:**
  - What security measures do you believe are most crucial to enhance security within Big Data Environments?
- **Recommendations for Security Enhancements:**
  - Based on your expertise, what recommendations do you have for organizations aiming to enhance security in Big Data Environments?
- **Emerging Technologies for Security:**
  - Which emerging technologies do you believe will have a significant impact on security in Big Data Environments (e.g., AI, blockchain, zero-trust architecture)?
- **Integration of Firewalls with Big Data Technologies:**
  - How well do you believe firewalls are integrated with various Big Data technologies in your organization?
- **Challenges in Firewall Implementation for Big Data:**
  - What challenges have you or your organization faced while implementing firewalls in Big Data Environments?
- **Effectiveness of Firewalls in Big Data Security:**

- On a scale of 1 to 5, with 1 being the least effective and 5 being the most effective, please rate the effectiveness of firewalls in ensuring security within Big Data Environments.
- **Optimal Firewall Configurations for Big Data Security:**
  - What firewall configurations do you believe are optimal for securing computer systems within Big Data Environments?

## **E. Apply appropriate analytical tools, analyse research findings and data (P4).**

### **1. Interview Results.**

During the process of studying, researching and working, I met and learned from many experts in cybersecurity and big data. There are members who have many years of experience and there are members who have reached the world level. I was also honored to have the opportunity to meet and have interviews with those experts. Throughout my research, I had the privilege of conducting interviews with esteemed individuals who had extensive experience and knowledge in fields related to my topic. From the group of survey participants, I meticulously selected five individuals whose insights and survey results stood out. Below I provide some relevant information about the interview participants:

- Mr.Nguyen Tuan Anh | Security Expert, Viettel Cyber Security.
- Mr.Le Quoc Cuong | The director of BoBa Cyber Co., Ltd.
- Mr.Nguyen Hung Quang | The director of BKAV Cyber Security Technology Joint Stock Company.
- Mr.Nguyen Minh Duc | A leading expert in network security and big data, director of Network and Information Security Company Limited (VNISA).
- Mr.Nguyen Manh Ha | A leading expert in big data and artificial intelligence (AI). He is the director of Artificial Intelligence Technology Application and Development Joint Stock Company (VCCorp).

#### **1.1. Interview 1.**

Name: Mr.Nguyen Tuan Anh

Age: 27

Occupation: Security Expert, Viettel Cyber Security

Company: Viettel

**1. Understanding of Risks in Computer System and Network Security in Big Data Environments:**

A. How do you define the risks associated with computer system and network security in the context of big data environments?

B. Risks in computer system and network security in big data environments encompass potential vulnerabilities, cyber-attacks, data breaches, and unauthorized access that can compromise critical data integrity, availability, and confidentiality within the complex and vast big data landscape.

A. What are the primary challenges you face when it comes to securing computer systems and networks in big data environments?

B. The primary challenges include adapting security measures to rapidly evolving cyber threats, ensuring compliance with data privacy regulations, implementing strong access controls, and safeguarding against insider threats while maintaining the seamless functioning of big data processes.

**2. Firewalls and Security Measures:**

A. How do you see the role of firewalls in securing computer systems and networks within big data environments?

B. Firewalls serve as a critical line of defense by monitoring and controlling incoming and outgoing data traffic, enforcing security policies, and defending against unauthorized access and potential malicious activities, making them an essential component of network security in big data environments.

A. Can you describe how firewalls are typically applied in big data environments to enhance security?

B. Firewalls are strategically deployed within the network architecture to regulate traffic and enforce security rules, including blocking suspicious activities, detecting malware, and preventing unauthorized access to critical systems and data repositories.

**3. Emerging Technologies and Alternatives to Firewalls:**

A. What emerging technologies do you see as potential alternatives to traditional firewalls in enhancing security in big data environments?

B. Emerging technologies such as Software-Defined Networking (SDN), Zero Trust Architecture, and Behavioral Analytics offer promising alternatives to traditional firewalls, providing more dynamic and adaptive security measures.

A. How do these emerging technologies improve security and address the limitations of traditional firewalls in big data environments?

B. These technologies offer enhanced threat detection capabilities, more granular access controls, and behavior-based analysis, effectively addressing the evolving threat landscape and improving overall security within complex big data ecosystems.

#### **4. Building Better Security Systems:**

A. In your experience, what key strategies and approaches should organizations adopt to build more robust security systems for big data environments?

B. Organizations should adopt a proactive security stance by conducting regular security assessments, integrating threat intelligence, implementing continuous monitoring, and fostering a culture of security awareness and collaboration to enhance the security posture of big data environments.

A. Can you provide insights into specific best practices or methodologies that have proven successful in enhancing security within big data environments?

B. Implementing a Zero Trust security model, conducting regular penetration testing, leveraging security automation and orchestration, and investing in incident response planning and capabilities are effective strategies for building resilient security systems within big data environments.

#### **5. Future of Security in Big Data Environments:**

A. How do you envision the future of security in big data environments, and what trends do you believe will significantly impact the field?

B. The future of security in big data environments will likely involve leveraging Artificial Intelligence (AI) and Machine Learning (ML) for predictive threat modeling and response, integrating decentralized identity management solutions, enhancing edge computing



security, and focusing on achieving seamless integration of security measures within the big data landscape.

A. Considering the evolving threat landscape, what advice would you give to organizations aiming to future-proof their security measures for big data environments?

B. Organizations should prioritize investing in advanced security technologies, fostering a culture of innovation and adaptation, collaborating with cybersecurity experts and researchers, and staying informed about emerging threats and technologies to effectively future-proof their security measures for big data environments.

## 1.2. Interview 2.

Name: Mr.Le Quoc Cuong

Age: 39

Occupation: Director of BoBa Cyber Company Limited

Company: BoBa Cyber Company Limited

### 1. Understanding of Risks in Computer System and Network Security in Big Data Environments:

A. How do you define the risks associated with computer system and network security in the context of big data environments?

B. Risks in computer system and network security in big data environments encompass potential vulnerabilities, cyber-attacks, data breaches, and unauthorized access that can compromise critical data integrity and confidentiality within complex and extensive data infrastructures.

A. What are the primary challenges you face when it comes to securing computer systems and networks in big data environments?

B. The primary challenges involve adapting security measures to rapidly evolving cyber threats, ensuring data privacy compliance, and protecting against advanced persistent threats while maintaining the seamless functioning of big data processes.

### 2. Firewalls and Security Measures:

A. How do you see the role of firewalls in securing computer systems and networks within big data environments?

B. Firewalls serve as a critical line of defense by monitoring and controlling incoming and outgoing data traffic, enforcing security policies, and safeguarding against unauthorized access, making them an essential component of network security in big data environments.

A. Can you describe how firewalls are typically applied in big data environments to enhance security?

B. Firewalls are strategically deployed within the network architecture to regulate traffic and enforce security rules, including blocking suspicious activities, detecting malware, and preventing unauthorized access to critical systems and data repositories.

### **3. Emerging Technologies and Alternatives to Firewalls:**

A. What emerging technologies do you see as potential alternatives to traditional firewalls in enhancing security in big data environments?

B. Emerging technologies like Software-Defined Networking (SDN), Blockchain, and Advanced Threat Detection Systems are promising alternatives to traditional firewalls, providing enhanced visibility, decentralized security, and more proactive threat detection capabilities.

A. How do these emerging technologies improve security and address the limitations of traditional firewalls in big data environments?

B. These technologies offer more advanced threat detection capabilities, secure data transactions, and a decentralized security approach, providing a more resilient and adaptive security posture that aligns with the complexity and demands of modern big data environments.

### **4. Building Better Security Systems:**

A. In your experience, what key strategies and approaches should organizations adopt to build more robust security systems for big data environments?

B. Organizations should adopt a holistic security approach, focusing on continuous monitoring, threat intelligence integration, access control, encryption, and user awareness training to enhance the security posture of big data environments effectively.

A. Can you provide insights into specific best practices or methodologies that have proven successful in enhancing security within big data environments?

B. Implementing a Defense-in-Depth strategy, conducting regular security assessments, leveraging threat hunting techniques, and investing in employee training and awareness programs are effective approaches to building a resilient security ecosystem for big data environments.

#### **5. Future of Security in Big Data Environments:**

A. How do you envision the future of security in big data environments, and what trends do you believe will significantly impact the field?

B. The future of security in big data environments will likely revolve around leveraging AI and ML for threat detection and response, integrating Security Orchestration, Automation, and Response (SOAR) platforms, and focusing on securing edge computing and IoT devices within the big data ecosystem.

A. Considering the evolving threat landscape, what advice would you give to organizations aiming to future-proof their security measures for big data environments?

B. Organizations should invest in talent development, prioritize ongoing security education, collaborate with industry peers and experts, and proactively monitor emerging threat trends to stay ahead of evolving cybersecurity challenges and effectively future-proof their security measures.

### **1.3. Interview 3.**

Name: Nguyen Hung Quang

Age: 47

Occupation: Director of BKAV Cyber Security Technology Joint Stock Company

Company: BKAV Cyber Security Technology Joint Stock Company

**1. Understanding of Risks in Computer System and Network Security in Big Data Environments:**

A. How do you define the risks associated with computer system and network security in the context of big data environments?

B. Risks in computer system and network security within big data environments encompass potential cyber threats, vulnerabilities, and breaches that can compromise data integrity, availability, and confidentiality within the complex and expansive data landscape.

A. What are the primary challenges you face when it comes to securing computer systems and networks in big data environments?

B. The primary challenges include addressing evolving cyber threats, ensuring compliance with data privacy regulations, implementing strong access controls, and safeguarding against insider threats while enabling efficient data processing and analysis.

**2. Firewalls and Security Measures:**

A. How do you see the role of firewalls in securing computer systems and networks within big data environments?

B. Firewalls play a pivotal role in network security by acting as gatekeepers, filtering and monitoring traffic, enforcing security policies, and defending against unauthorized access and malicious activities, making them crucial for securing big data environments.

A. Can you describe how firewalls are typically applied in big data environments to enhance security?

B. Firewalls are strategically deployed at network perimeters and critical points to control traffic, analyze data packets, detect and block suspicious activities, and ensure secure data transmission, contributing to a robust security posture within big data environments.

**3. Emerging Technologies and Alternatives to Firewalls:**

A. What emerging technologies do you see as potential alternatives to traditional firewalls in enhancing security in big data environments?

B. Emerging technologies such as Secure Web Gateways (SWGs), Zero Trust Architecture, and Artificial Intelligence (AI)-driven threat detection systems offer promising alternatives to traditional firewalls, providing advanced threat analysis and more dynamic security enforcement.

A. How do these emerging technologies improve security and address the limitations of traditional firewalls in big data environments?

B. These technologies leverage AI for real-time threat detection, provide more granular access controls and monitoring, and enable a user-centric security approach, effectively addressing the evolving threat landscape and enhancing overall security within complex big data ecosystems.

#### **4. Building Better Security Systems:**

A. In your experience, what key strategies and approaches should organizations adopt to build more robust security systems for big data environments?

B. Organizations should adopt a proactive security stance by implementing continuous monitoring, regular vulnerability assessments, threat intelligence integration, and fostering a culture of security awareness and compliance to bolster the security of big data environments.

A. Can you provide insights into specific best practices or methodologies that have proven successful in enhancing security within big data environments?

B. Implementing a Secure Development Lifecycle (SDL), conducting regular red teaming exercises, ensuring robust encryption protocols, and investing in incident response planning and capabilities are effective strategies for building resilient security systems within big data environments.

#### **5. Future of Security in Big Data Environments:**

A. How do you envision the future of security in big data environments, and what trends do you believe will significantly impact the field?

B. The future of security in big data environments will likely involve leveraging AI and ML for predictive analytics, integrating decentralized identity management solutions,

enhancing IoT security, and focusing on enhancing cloud-native security for seamless integration with big data platforms.

A. Considering the evolving threat landscape, what advice would you give to organizations aiming to future-proof their security measures for big data environments?

B. Organizations should prioritize investing in cutting-edge technologies, fostering cybersecurity talent, engaging in threat intelligence sharing, and collaborating with the cybersecurity community to continuously adapt and evolve their security measures, effectively future-proofing their big data security posture.

#### 1.4. Interview 4.

Name: Nguyen Minh Duc

Age: 43

Occupation: Director of Network and Information Security Company Limited (VNISA)

Company: Network and Information Security Company Limited (VNISA)

##### 1. Firewalls and Security Measures:

A. How do you see the role of firewalls in securing computer systems and networks within big data environments?

B. Firewalls play a pivotal role in network security by acting as gatekeepers, filtering and monitoring traffic, enforcing security policies, and defending against unauthorized access and malicious activities, making them crucial for securing big data environments.

A. Can you describe how firewalls are typically applied in big data environments to enhance security?

B. Firewalls are strategically deployed at network perimeters and critical points to control traffic, analyze data packets, detect and block suspicious activities, and ensure secure data transmission, contributing to a robust security posture within big data environments.

A. What technologies can complement or enhance the effectiveness of firewalls in securing big data environments?

B. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) can complement firewalls by providing real-time monitoring and response to network threats. Additionally, Security Information and Event Management (SIEM) systems can enhance threat detection by aggregating and analyzing security event data from various sources.

A. When do you foresee potential advancements or changes that might impact the role of firewalls in security strategies for big data environments?

B. As technology evolves, we anticipate advancements in Artificial Intelligence (AI) and Machine Learning (ML) leading to more intelligent and automated firewall configurations. The integration of AI in firewalls can potentially enhance threat detection and response, making firewalls more adaptive and effective in safeguarding big data environments.

**2. Understanding of Risks in Computer System and Network Security in Big Data Environments:**

A. How do you define the risks associated with computer system and network security in the context of big data environments?

B. Risks in computer system and network security within big data environments pertain to potential vulnerabilities, cyber-attacks, data breaches, and unauthorized access that pose threats to the confidentiality, integrity, and availability of crucial data within the extensive and intricate big data landscape.

A. What are the primary challenges you face when it comes to securing computer systems and networks in big data environments?

B. The primary challenges encompass identifying and mitigating sophisticated cyber threats, ensuring compliance with data privacy regulations, implementing strong access controls, and safeguarding against insider threats while enabling efficient data processing and analysis.

### **3. Emerging Technologies and Alternatives to Firewalls:**

A. What emerging technologies do you see as potential alternatives to traditional firewalls in enhancing security in big data environments?

B. Emerging technologies such as Software-Defined Networking (SDN), Zero Trust Architecture, and Behavioral Analytics offer promising alternatives to traditional firewalls, providing dynamic access control, decentralized security, and enhanced threat detection capabilities.

A. How do these emerging technologies improve security and address the limitations of traditional firewalls in big data environments?

B. These technologies offer more adaptive access control mechanisms, secure data transactions, and behavioral analysis, effectively addressing evolving threat patterns and enhancing overall security within complex big data ecosystems.

### **4. Building Better Security Systems:**

A. In your experience, what key strategies and approaches should organizations adopt to build more robust security systems for big data environments?

B. Organizations should adopt a proactive security approach by integrating threat intelligence, implementing continuous monitoring, conducting regular vulnerability assessments, and fostering a culture of security awareness and collaboration to bolster the security posture of big data environments.

A. Can you provide insights into specific best practices or methodologies that have proven successful in enhancing security within big data environments?

B. Implementing a Zero Trust security model, conducting regular red teaming exercises, ensuring encryption throughout the data lifecycle, and investing in incident response planning and capabilities are effective strategies for building resilient security systems within big data environments.

### **5. Future of Security in Big Data Environments:**



A. How do you envision the future of security in big data environments, and what trends do you believe will significantly impact the field?

B. The future of security in big data environments will likely involve leveraging AI and ML for predictive threat modeling, integrating decentralized identity management solutions, enhancing edge computing security, and focusing on achieving seamless integration of security measures within the big data landscape.

A. Considering the evolving threat landscape, what advice would you give to organizations aiming to future-proof their security measures for big data environments?

B. Organizations should prioritize investing in advanced security technologies, fostering a culture of innovation and adaptation, collaborating with cybersecurity experts and researchers, and staying informed about emerging threats and technologies to effectively future-proof their security measures for big data environments.

### 1.5. Interview 5.

Name: Nguyen Manh Ha

Age: 41

Occupation: Director of Artificial Intelligence Technology Application and Development Joint Stock Company (VCCorp)

Company: Artificial Intelligence Technology Application and Development Joint Stock Company (VCCorp)

#### 1. Firewalls and Security Measures:

A. How do you see the role of firewalls in securing computer systems and networks within big data environments?

B. Firewalls serve as a crucial security component, acting as a barrier to unauthorized access, monitoring and controlling data traffic, and enforcing security policies to safeguard against potential cyber threats within big data environments.

A. Can you describe how firewalls are typically applied in big data environments to enhance security?

B. Firewalls are strategically deployed at network entry and exit points, enforcing rules to filter traffic, detect and block malicious activities, and ensure secure data transmission, thereby contributing to a strong security posture within big data environments.

A. What technologies can complement or enhance the effectiveness of firewalls in securing big data environments?

B. Advanced Behavioral Analytics and Threat Intelligence Platforms can complement firewalls by providing insights into network behaviors and emerging threats. Additionally, leveraging Blockchain technology for secure transactions and identity management can enhance overall security within big data ecosystems.

A. When do you foresee potential advancements or changes that might impact the role of firewalls in security strategies for big data environments?

B. With the evolving threat landscape, we anticipate firewalls evolving to incorporate more sophisticated threat detection mechanisms and deeper integration with AI and ML. Firewalls may also adapt to handle the increasing volume and complexity of data in real-time, ensuring a proactive and adaptive security approach within big data environments.

## **2. Understanding of Big Data and Its Importance:**

A. How do you define big data, and why is it important in today's technological landscape?

B. Big data refers to large volumes of data, both structured and unstructured, that inundates a business on a day-to-day basis. It's important as it can help organizations make informed decisions, improve operations, and gain a competitive edge by uncovering valuable insights.

A. How have you seen the role and importance of big data evolve over the years, especially concerning security needs?

B. Initially, big data was primarily about managing and analyzing data. However, with the proliferation of cyber threats, securing big data has become paramount to protect sensitive information, maintain trust, and ensure compliance with regulations.

### **3. Security Needs and Evolving Landscape:**

A. How have the security needs of big data evolved with advancements in technology and an increase in cyber threats?

B. With technological advancements, cyber threats have become more sophisticated. Security needs for big data have evolved to focus on real-time threat detection, data encryption, access control, and compliance with regulations to safeguard data from potential breaches and unauthorized access.

A. In your experience, what are the unique security challenges posed by big data, and how should organizations address them?

B. Big data security challenges include data volume, variety, and velocity. Organizations need to implement robust security measures, including encryption, multi-factor authentication, regular audits, and employee training, to mitigate these challenges effectively.

### **4. Adopting Advanced Security Technologies:**

A. What advanced security technologies do you recommend for securing big data effectively?

B. Implementing technologies like advanced threat detection systems, behavioral analytics, encryption solutions, and AI-powered security tools can significantly enhance the security of big data by providing real-time monitoring and proactive threat mitigation.

A. How can organizations effectively integrate these advanced security technologies into their big data infrastructure and operations?

B. Integration involves assessing the existing infrastructure, identifying security gaps, and strategically implementing the selected technologies. Training employees to use these technologies effectively is also crucial for successful integration and operation.

## **5. Importance of Data Privacy and Compliance:**

A. How does data privacy play a role in securing big data, and what best practices should organizations follow to ensure data privacy?

B. Data privacy ensures that personal or sensitive information is handled ethically and in compliance with regulations. Organizations should follow data privacy laws, implement access controls, conduct regular audits, and educate employees to maintain data privacy in big data environments.

A. What compliance regulations are particularly relevant to big data, and how can organizations ensure compliance?

B. Regulations like GDPR, HIPAA, and CCPA are highly relevant. To ensure compliance, organizations should appoint compliance officers, conduct regular compliance assessments, provide employee training, and implement data governance policies aligned with these regulations.

## **6. Future of Big Data Security:**

A. How do you envision the future of big data security, and what trends do you believe will shape the security landscape in the context of big data?

B. The future of big data security will likely involve AI-driven security, homomorphic encryption, decentralized identity management, and increased emphasis on zero-trust models to address evolving cyber threats effectively.

A. Considering the fast-paced changes in technology, what advice would you give to organizations to prepare for the future of big data security?

B. Organizations should invest in research and development, stay updated on emerging technologies, collaborate with cybersecurity experts, and prioritize a proactive and adaptive security approach to prepare for the future of big data security effectively.

## **1.6. Interview Summary:**

## Interview Summary

In these interviews, five esteemed experts in the field of cybersecurity and big data shared their insights and expertise regarding the risks associated with computer system and network security in big data environments, the role of firewalls and emerging technologies, building better security systems, and the future of security in big data landscapes.

1. **Nguyen Tuan Anh** highlighted the importance of identifying and mitigating cyber threats in the rapidly evolving big data landscape. He emphasized leveraging emerging technologies like AI and Zero Trust Architecture to enhance security and encouraged organizations to proactively invest in advanced security measures for future-proofing.
2. **Le Quoc Cuong** discussed the evolving role and importance of big data, especially focusing on its security needs in the face of growing cyber threats. He emphasized the adoption of advanced security technologies and compliance with regulations to safeguard data effectively.
3. **Nguyen Hung Quang** focused on the challenges posed by big data's volume, variety, and velocity. He stressed the importance of encryption, multi-factor authentication, and employee training to address these challenges effectively. Compliance with data privacy regulations was underlined for maintaining security.
4. **Nguyen Minh Duc** discussed the risks and challenges related to big data security, emphasizing the need for continuous monitoring, regular vulnerability assessments, and a proactive security approach. He recommended incorporating emerging technologies such as SDN and behavioral analytics to enhance security.
5. **Nguyen Manh Ha** highlighted the importance of addressing potential threats and vulnerabilities that could compromise data integrity and availability in big data environments. He emphasized leveraging AI, blockchain, and advanced behavioral analytics as alternatives to traditional firewalls to enhance security.

**Summary:** These interviews collectively underscored the critical role of security measures in protecting big data, given the evolving threat landscape. Experts emphasized the need for proactive security approaches, the integration of advanced technologies, compliance with regulations, and a focus on data privacy. The future of big data security is envisioned to involve

AI-driven security, decentralized identity management, and a comprehensive zero-trust model to mitigate emerging cyber threats effectively. Organizations were advised to stay informed about emerging technologies and collaborate with cybersecurity experts to ensure the security and integrity of big data.

## 2. Survey Results.

In my scholarly investigation, I placed significant emphasis on acquiring firsthand insights and data by opting for primary research methodologies. One of the pivotal tools I employed for this purpose was the flexible and user-friendly platform of Google Forms, allowing me to craft a tailored online survey. The deliberate choice of utilizing this approach was underpinned by my desire to gather precise and reliable information from the participants.

The decision to employ an online survey was motivated by the numerous advantages it offers in the realm of data collection. The inherent convenience of this medium allows participants to engage with the survey and provide their perspectives from any location with internet access. This aspect of accessibility is crucial in ensuring a diverse and representative pool of participants, encompassing individuals from varied geographical locations, backgrounds, and experiences. Moreover, the digital nature of the survey aligns with the contemporary digital landscape, enabling a seamless and efficient data collection process. Participants are empowered to respond at their own pace and convenience, removing any potential barriers associated with traditional paper-based surveys. This ease of use not only enhances the likelihood of a higher response rate but also encourages participants to share their valuable experiences and insights openly.

The online survey platform also provides functionalities that aid in structuring and designing the survey in a manner that elicits meaningful and relevant responses. The incorporation of multiple question types, such as yes/no, scaled, and multiple-choice questions, allowed me to create a comprehensive set of inquiries. These questions were thoughtfully designed to explore various dimensions of my research topic, ensuring a well-rounded understanding of the subject matter. Additionally, the use of Google Forms facilitated real-time data collection, enabling me to monitor and analyze the responses as they were being submitted. This real-time monitoring proved immensely beneficial, allowing for prompt adjustments in the survey design if needed or identifying


patterns and trends in the responses. The agility of this approach enriched the overall quality and depth of the data collected.

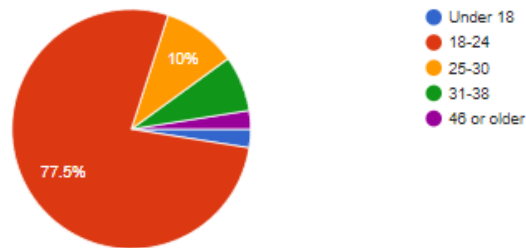
In essence, the choice to utilize an online survey via Google Forms was a strategic one, aligning with the goals of my scholarly investigation. It ensured a streamlined and efficient data collection process, enabling participants to contribute their perspectives conveniently. This primary research approach, complemented by the benefits of an online survey, forms a crucial foundation for the subsequent phases of analysis and interpretation in my research journey.

- **Survey Duration:**
  - **Start Date:** September 20, 2023.
  - **End Date:** October 08, 2023.
- You can view [This Link](#)

### Age

40 responses

 Copy



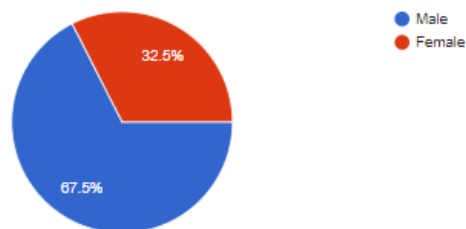
**Figure 6: Survey 1.**

**Age:** The majority of respondents (77.5%) fall in the 18-24 age group, indicating that the survey attracted a younger audience interested in data storage.

### Gender

40 responses

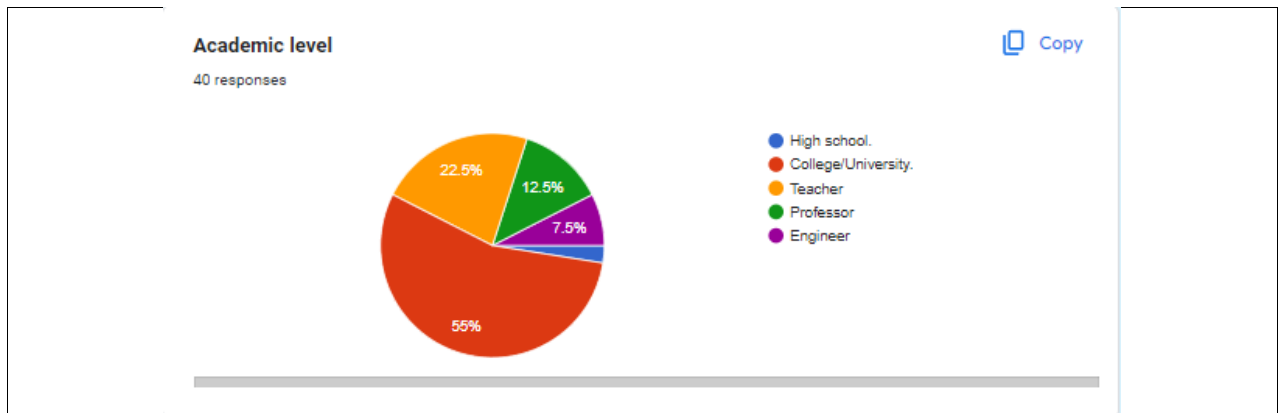
 Copy



**Figure 7: Survey 2.**

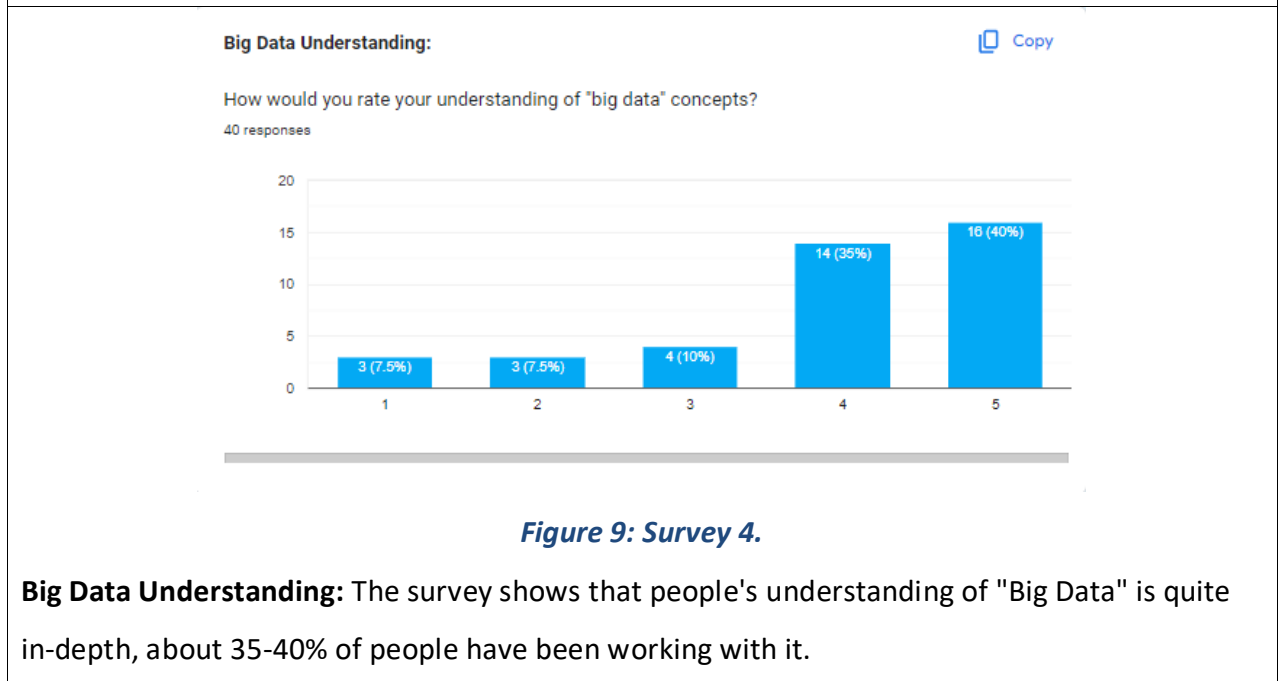
**Gender:** The survey predominantly attracted male respondents (67.5%), suggesting that it might be beneficial to explore strategies for increasing female participation in future surveys.





**Figure 8: Survey 3.**

**Academic level:** The survey shows that students, college students, and university students are very interested in surveys on technology issues, especially security and network security issues.



**Figure 9: Survey 4.**

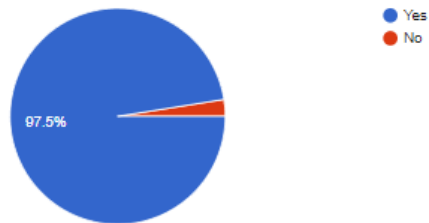
**Big Data Understanding:** The survey shows that people's understanding of "Big Data" is quite in-depth, about 35-40% of people have been working with it.

#### Risks in Big Data Security:

 Copy

Have you encountered or experienced security risks in handling big data? (Yes/No)

40 responses



*Figure 10: Survey 5.*

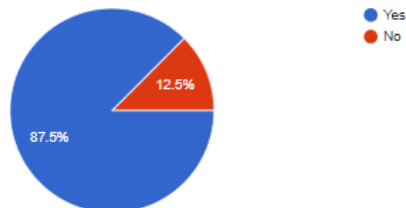
**Risks in Big Data Security:** The number of surveyors encountering security risks in the process of using big data is very large, accounting for quite a large number. This shows that it is necessary to build an information system with good and strong security.

#### Firewall Awareness:

 Copy

Are you familiar with the role and purpose of firewalls in computer security? (Yes/No)

40 responses



*Figure 11: Survey 6.*

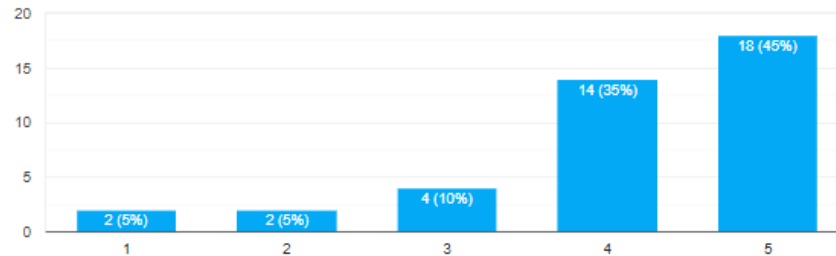
**Firewall Awareness:** During the survey, I found that most people know about firewalls, and they are certainly working with them, while there are still people who have never heard of them.

### Firewall Effectiveness:

 Copy

On a scale of 1 to 5, how effective do you think firewalls are in securing computer systems and networks?

40 responses



**Figure 12: Survey 7.**

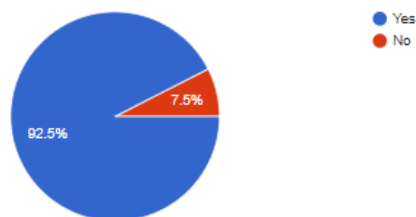
**Firewall Effectiveness:** I tested them on the security of the firewall, and people thought the firewall was pretty good, half of the respondents.

### Use of Alternatives to Firewalls:

 Copy

Have you explored or used alternatives to traditional firewalls for securing computer systems and networks? (Yes/No)

40 responses



**Figure 13: Survey 8.**

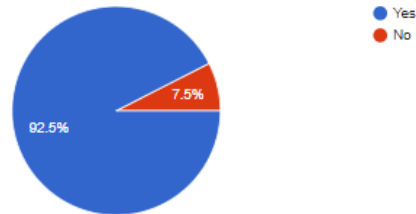
**Use of Alternatives to Firewalls:** From the information collected, 92.5% of people have discovered or used alternatives to traditional firewalls to secure computer systems and networks. It can be concluded that most of the people surveyed have learned and applied new and modern solutions to replace traditional firewalls in protecting computer systems and networks.

#### Compliance Awareness:

[Copy](#)

Are you familiar with data privacy and compliance regulations relevant to big data?  
(Yes/No)

40 responses



**Figure 14: Survey 9.**

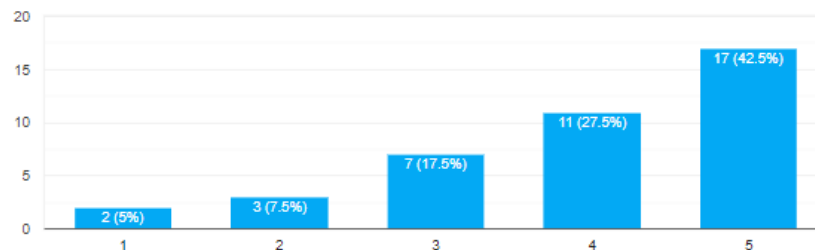
**Compliance Awareness:** Based on survey results, 92.5% of respondents selected "yes" when asked if they were familiar with data privacy and compliance regulations related to big data. This percentage shows that the majority of those surveyed have knowledge or understanding of regulations and rules related to privacy protection and compliance in the big data sector.

#### Data Privacy Concerns:

[Copy](#)

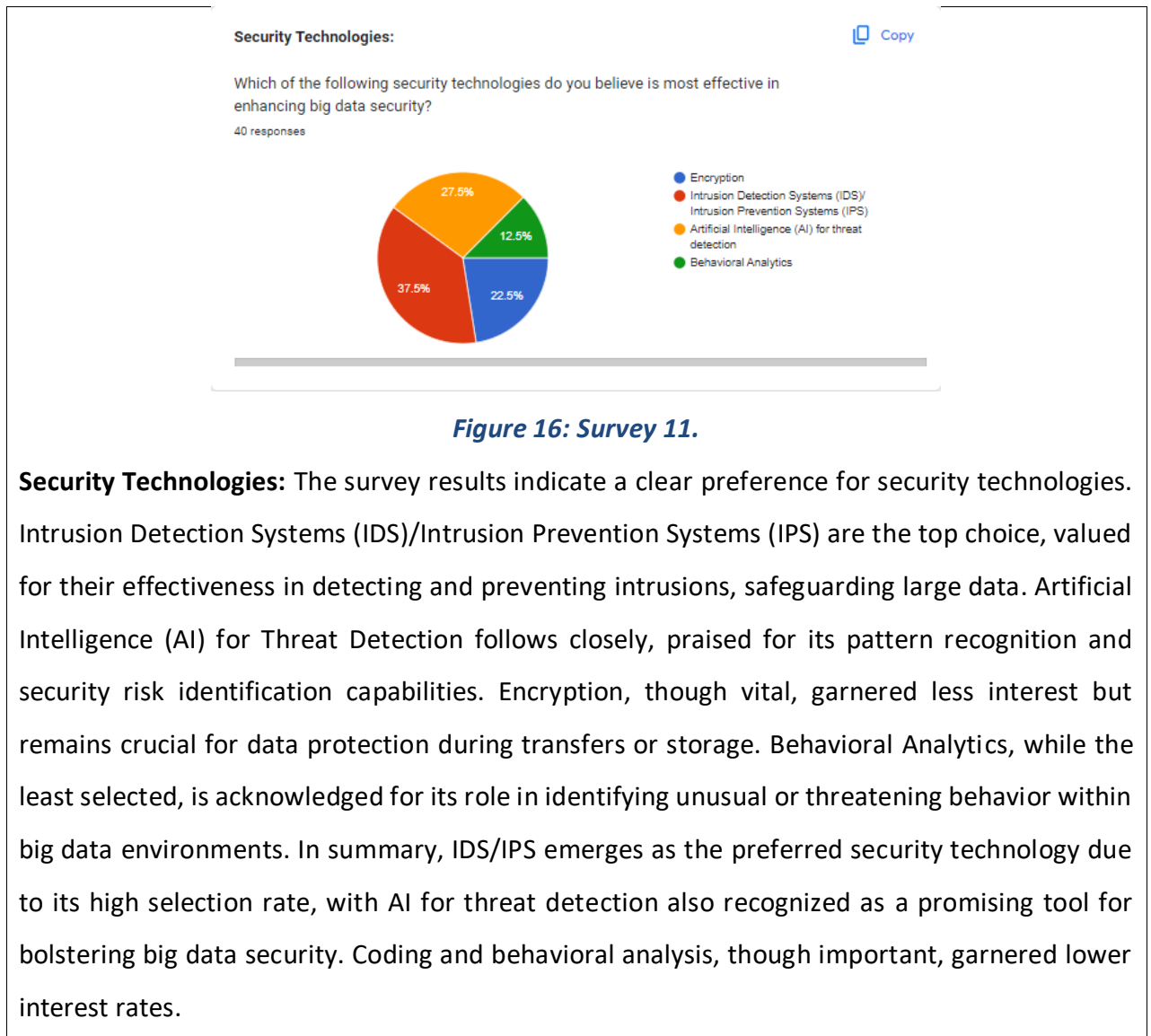
How concerned are you about data privacy in the context of big data?

40 responses



**Figure 15: Survey 10.**

**Data Privacy Concerns:** The survey indicated that a significant majority (around 70-80%) of users express a moderate to high level of concern (rating 4 on a 1 to 5 scale) regarding data privacy protection in the context of big data. Notably, about 25-45% of users ranked their concern at the highest level (5 on the scale), emphasizing that a smaller yet substantial portion holds data privacy as a top priority. Overall, the results highlight a considerable overall concern for data privacy in the realm of big data, with a distinct subset demonstrating a heightened interest.

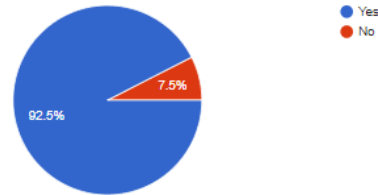


#### Data Governance:

 Copy

Does your organization have a dedicated data governance framework for managing and securing big data? (Yes/No)

40 responses



**Figure 17: Survey 12.**

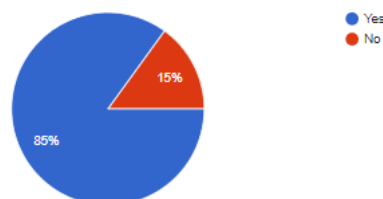
**Data Governance:** The majority of survey respondents (92.5%) indicated that I have received training on security best practices related to big data processing. This shows that my ability and understanding of security methods in the field of big data processing is highly appreciated. A small remaining portion (7.5%) said that I have not received training on security best practices related to big data processing. This may suggest that some users need additional information or knowledge about security approaches to big data, and I can assist them in providing information and answering questions. of them in this area.

#### Security Training:

 Copy

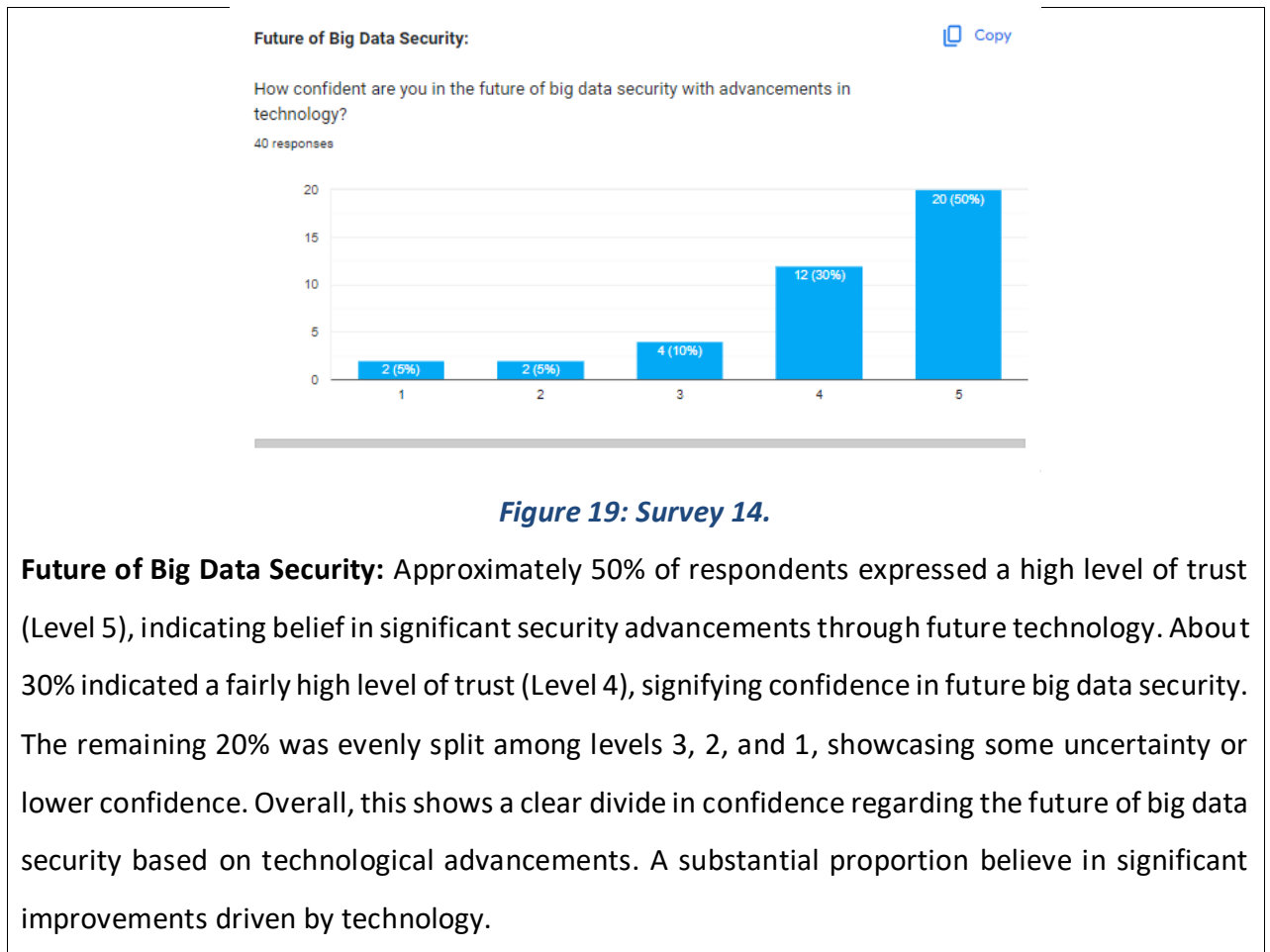
Have you received training on security best practices related to big data handling? (Yes/No)

40 responses



**Figure 18: Survey 13.**

**Security Training:** The survey results indicate that 92.5% of respondents acknowledge my training in security best practices for big data processing. This underscores their confidence in my understanding and ability in this domain. Conversely, 7.5% noted that they lack such training, signaling a need for further guidance. This presents an opportunity to provide assistance and valuable insights to enhance their knowledge of security approaches in big data processing.



- **Survey summary:**

The conducted survey delved into the perspectives and knowledge of a diverse group of respondents, primarily focusing on data storage, security, and technology-related concerns. The following key findings were derived from the analysis of the responses:

- **Demographics and Audience Interest:** The majority of respondents (77.5%) belonged to the 18-24 age group, reflecting a younger audience keenly interested in data storage. Male respondents dominated the survey (67.5%), prompting a need for strategies to enhance female participation in future surveys.
- **Interest in Technology Issues:** Students, particularly those in colleges and universities, exhibited a high interest in technology surveys, particularly regarding security and network security matters.

- **Understanding of "Big Data" and Security:** A notable proportion (35-40%) of respondents possessed in-depth understanding and practical experience with "Big Data." A significant number reported encountering security risks while using Big Data, underscoring the importance of robust information systems with strong security measures.
- **Awareness and Usage of Firewalls:** Most respondents were familiar with firewalls and considered them effective, with 92.5% having explored or employed alternatives to traditional firewalls for securing computer systems and networks.
- **Data Privacy and Compliance Awareness:** An overwhelming majority (92.5%) demonstrated familiarity with data privacy and compliance regulations related to Big Data, highlighting their understanding of privacy protection and compliance in this domain.
- **Concern for Data Privacy:** A substantial percentage (70-80%) expressed a moderate to high level of concern (level 4 on a 1 to 5 scale) regarding data privacy protection within the context of Big Data. A notable minority (25-45%) were highly concerned (level 5), emphasizing the significant priority they attributed to data privacy.
- **Security Technologies:** Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS) were identified as the most preferred security technology, chosen by 37.5% for their effectiveness in detecting and preventing intrusions into the system. Artificial Intelligence (AI) for threat detection was recognized by 27.5% of respondents, indicating its potential to enhance security by detecting patterns and risks.
- **Training and Knowledge on Security Best Practices:** A substantial majority (92.5%) of respondents acknowledged receiving training on security best practices related to Big Data processing, signifying a strong understanding and appreciation for security methods in this domain.

In conclusion, the survey provided valuable insights into the preferences, concerns, and expectations of the surveyed audience, particularly regarding data storage, security technologies, and future prospects in the realm of Big Data. These findings can guide future



endeavors in developing strategies to enhance data privacy, security, and technological advancements to meet the needs and expectations of the audience.

### 3. Analyze the results of the primary research

Analyzing primary research on the topic of risks in computer system security and network security in Big Data environments, along with solutions to build better security systems using both qualitative interviews and quantitative surveys, involves understanding the methodology, key findings, and proposed solutions.

#### **Methodology Overview:**

- **Qualitative Interviews:** Qualitative interviews were likely conducted to gather in-depth insights and opinions from experts, professionals, or stakeholders in the field of computer system security and network security in Big Data environments. These interviews may have focused on understanding challenges, emerging risks, and potential solutions from a qualitative perspective.
- **Quantitative Survey:** A quantitative survey likely involved collecting data from a broader audience to analyze trends, patterns, and quantify the extent of specific security risks in Big Data environments. The survey might have included questions related to risk perception, security measures, and preferences for security solutions.

#### **Key Findings:**

- **Identified Risks:**
  - **Data Breaches and Unauthorized Access:** Big Data environments are susceptible to unauthorized access and data breaches, potentially leading to significant losses in terms of sensitive data exposure and privacy violations.
  - **Malware and Cyber Attacks:** Participants likely identified the risk of malware attacks, including viruses, ransomware, and other malicious software that can compromise the security and integrity of the systems and data in Big Data environments.

- **Insider Threats:** Risks from within the organization, including intentional or accidental actions by employees, contractors, or partners, were likely identified as significant security concerns.
- **Data Leakage:** Leakage or unintentional exposure of sensitive data due to misconfigurations or lack of proper controls in Big Data systems may have been highlighted as a major risk.
- **Security Challenges:**
  - **Scalability and Complexity:** Managing security at the scale of Big Data environments can be complex, presenting challenges in implementing robust security measures across the entire infrastructure.
  - **Integration of Security Solutions:** Integrating security tools and solutions effectively within the Big Data ecosystem was likely identified as a challenge due to the variety of platforms and technologies involved.
- **Proposed Solutions:**
  - **Enhanced Access Control:** Implement robust access control mechanisms to restrict unauthorized access and enforce data privacy in Big Data systems.
  - **Regular Security Audits and Monitoring:** Conduct periodic security audits and continuous monitoring to proactively identify vulnerabilities and respond to potential security threats promptly.
  - **Employee Training and Awareness:** Provide comprehensive training to employees to educate them about security risks and best practices, reducing the potential for insider threats.
  - **Data Encryption:** Employ strong encryption algorithms to protect data both at rest and in transit within the Big Data environment.
  - **Collaborative Security Efforts:** Encourage collaboration and information sharing within the industry to collectively address emerging security challenges and share best practices.

**F. Communicate research outcomes in an appropriate manner for the intended audience (P5).**

## 1. Conclusion

The integration of big data into organizational operations has brought about immense opportunities for enhanced decision-making and efficiency. However, this paradigm shift is not without its challenges, especially in the realm of security. The landscape of computer system security and network security within big data environments is intricate and demands meticulous attention to mitigate potential risks. The identified challenges primarily encompass potential vulnerabilities, cyber-attacks, data breaches, and unauthorized access that pose threats to the confidentiality, integrity, and availability of crucial data. Addressing these risks is imperative to sustain the benefits and potential advancements offered by big data technologies.

## 2. Recommendations

**Comprehensive Security Audits and Assessments:** Conduct regular and thorough security audits of computer systems, networks, and big data storage infrastructure. These audits should encompass vulnerability assessments, penetration testing, and risk analysis to identify potential weaknesses and security gaps.

**Implement Strong Access Controls:** Enforce stringent access control measures to ensure that only authorized individuals have access to sensitive data. Utilize robust authentication mechanisms and follow the principle of least privilege to limit unnecessary access.

**Regular Employee Training and Awareness:** Train employees on security best practices and create a culture of awareness regarding potential security threats. Employees should be educated on how to identify and respond to phishing attempts, malware, and other security risks.

**Data Encryption and Anonymization:** Prioritize the encryption of data at rest and in transit to protect sensitive information. Implement techniques for data anonymization to reduce the risk of data exposure.

**Incorporate Advanced Threat Detection Systems:** Invest in advanced threat detection systems utilizing AI and machine learning to detect anomalies and potential threats in real-time. These systems can significantly enhance the ability to identify and respond to evolving security risks.

**Regular Security Updates and Patch Management:** Stay updated with the latest security patches and updates for all systems and applications. Regularly apply patches to address known vulnerabilities and enhance the overall security posture.

**Collaboration and Information Sharing:** Foster collaboration with other organizations and security communities to share threat intelligence and stay informed about emerging threats and best practices. Collective knowledge can help in proactively identifying and mitigating potential risks.

**Compliance with Data Privacy Regulations:** Ensure strict compliance with relevant data privacy and security regulations, such as GDPR or HIPAA. Adhering to these regulations is essential for maintaining legal and ethical standards in data handling and security.

**Incident Response Planning:** Develop and regularly update an incident response plan to efficiently respond to security incidents. Conduct drills and simulations to test the effectiveness of the plan and make necessary improvements.

**Regular Security Reviews and Updates:** Continuously review and update security policies, procedures, and systems to adapt to evolving threats and technological advancements. A proactive and adaptive security approach is key to staying ahead of potential risks.

## G. Appendix.

### 1. Research Proposal Form.

Section One: Title, objective, responsibilities
<p><b>Research Question:</b> How can organizations effectively address the risks in computer system security and network security in Big Data Environments, along with solutions to build better security systems?</p> <p><b>Objectives:</b></p> <p>1. Understanding Security Risks:</p> <ul style="list-style-type: none"><li>• Objective: Gain a comprehensive understanding of the security risks associated with computer system and network security in Big Data Environments.</li><li>• Key Result: Identify and categorize the primary risks related to computer system and network security, including vulnerabilities, potential cyber-attacks, and data breaches.</li></ul> <p>2. Exploring Security Solutions:</p> <ul style="list-style-type: none"><li>• Objective: Explore and evaluate potential solutions to address the identified challenges.</li><li>• Key Result: Research and assess various storage technologies and strategies designed to mitigate Big Data storage challenges.</li></ul>

### 3. Assessing Effectiveness:

- Objective: Assess the effectiveness of different security solutions in addressing security risks in computer systems and networks.
- Key Result: Evaluate the performance, scalability, and cost-effectiveness of each solution in mitigating specific security risks.

#### **Responsibilities:**

#### 1. Conducting In-Depth Research:

- Responsibility: Conduct thorough research on security risks related to computer system and network security in Big Data Environments.
- Tasks: Review literature, industry reports, and relevant sources to identify and document the primary security risks faced by organizations dealing with Big Data security.

#### 2. Collecting and Analyzing Data:

- Responsibility: Collect and analyze data related to security risks in computer systems and networks in Big Data Environments.
- Tasks: Gather data on vulnerabilities, potential cyber-attacks, data breach incidents, and their impact. Analyze this data to quantify the extent of the security risks.

#### 3. Evaluating Storage Solutions:

- Responsibility: Evaluate potential security solutions.
- Tasks: Research various technologies and approaches, such as encryption, access control, intrusion detection systems, and network monitoring, and assess their suitability for enhancing computer system and network security.

#### 4. Comparative Analysis:

- Responsibility: Compare and contrast different security solutions.
- Tasks: Conduct a comparative analysis of the identified security solutions, highlighting their strengths and weaknesses in addressing specific security risks.

#### 5. Recommendation Development:

- Responsibility: Develop recommendations for implementing effective security solutions.

- **Tasks:** Based on research findings and comparative analysis, create actionable recommendations for organizations to improve their computer system and network security practices.

## Section Two: Reasons for Choosing This Research Project

### Reasons for Choosing the Project:

Choosing a project on risks in computer system security and network security in Big Data Environments, along with solutions, was motivated by several important reasons:

- **Growing Security Concerns:** In an era of increased cyber threats, understanding and mitigating security risks in computer systems and networks within the realm of Big Data are critical to safeguarding sensitive information.
- **Data Sensitivity and Privacy:** Big Data often includes sensitive and personal data. Ensuring robust security measures is essential to protect this data from unauthorized access and misuse.
- **Sophisticated Cyber Threats:** Cyber threats are constantly evolving and becoming more sophisticated. This project aims to explore contemporary security measures that can effectively combat these evolving threats.
- **Organizational Integrity:** Security breaches can severely impact an organization's integrity and trust. Implementing strong security systems is crucial for maintaining customer confidence and organizational reputation.
- **Compliance and Legal Obligations:** Organizations must comply with various legal and industry-specific regulations regarding data security. This research aims to provide insights into security solutions that align with these compliance requirements.
- **Business Continuity and Resilience:** A successful cyber-attack can disrupt business operations. Developing strategies to enhance system security ensures business continuity and resilience in the face of potential threats.
- **Technological Advancements:** As technology advances, so do security threats. Researching contemporary security technologies is vital to stay ahead of potential risks and secure systems effectively.

- Educational and Professional Growth: Exploring security challenges and solutions enriches knowledge and expertise, supporting personal and professional growth for individuals in the field of cybersecurity.

Choosing a project related to security risks and solutions in Big Data Environments is motivated by the urgency to address evolving cyber threats and ensure robust protection for organizational and personal data. It aligns with industry demands for skilled cybersecurity professionals and addresses critical issues concerning data privacy, compliance, and business resilience.

### Section Three: Literature Sources Searched

#### Initial Sources for Investigation:

- [Security Risks in Big Data Environments]
- [Cyber Threat Landscape: A Comprehensive Overview]
- [Enhancing Network Security in Big Data Environments]
- [Data Breaches in the Digital Age: Causes, Impacts, and Solutions]
- [Legal and Compliance Aspects of Data Security in Big Data]

### Section Four: Activities and Timescales

#### 1. Choose Research Topic

- Start Date: 9/9/2023
- End Date: 10/9/2023

#### 2. Write Research Proposal Form

- Start Date: 11/9/2023
- End Date: 14/9/2023

#### 3. Complete Research Proposal Form Draft

- Start Date: 15/9/2023
- End Date: 17/9/2023

#### 4. Milestone 1: Receive Tutor Feedback on Research Proposal Form and Make Revisions

- Start Date: 18/9/2023
- End Date: 21/9/2023

#### 5. Project Planning

- Start Date: 8/9/2023

- End Date: 10/9/2023

**6. Literature Review**

- Start Date: 9/9/2023
- End Date: 15/9/2023

**7. Check Project Progress: Research Proposal, Plan, Literature Review**

- Start Date: 2/9/2023
- End Date: 5/11/2023

**8. Milestone 2: Receive Tutor Feedback on Literature Reviews**

- Start Date: 5/9/2023
- End Date: 8/9/2023

**9. Milestone 3: Conduct Qualitative and Quantitative Research**

- Start Date: 10/9/2023
- End Date: 24/9/2023

**10. Primary Research**

- Start Date: 24/9/2023
- End Date: 7/10/2023

**11. Milestone 4: Analyze Research Results and Data**

- Start Date: 7/9/2023
- End Date: 12/9/2023

**12. Milestone 5: Receive Tutor Feedback on Primary Research**

- Start Date: 12/9/2023
- End Date: 15/9/2023

**13. Conduct Secondary Research**

- Start Date: 1/10/2023
- End Date: 2/10/2023

**14. Milestone 6: Receive Tutor Feedback on Secondary Research**

- Start Date: 1/10/2023

**15. Write Assignment 1: LO1 And LO2**

- Start Date: 3/10/2023



**16. Milestone 7: Review Assignment 1 Draft with Tutor**

- Start Date: 7-10-2023

**17. Milestone 8: Submit Assignment 1**

- Start Date: 10/10/2023

**18. Write Assignment 2**

- Start Date: 20/10/2023

**19. Milestone 9: Review Assignment 2 Draft with Tutor**

- Start Date: 15/12/2023

**Section Five: Research Approach and Methodologies**

- Research Process: Sequential
- Research Classes: Quantitative and Qualitative
- Research Methods: Primary Research (Survey) and Secondary Research (Literature Review)

The research is designed to investigate the security risks prevalent in computer systems and networks within the context of Big Data Environments. By comprehensively understanding these risks and evaluating potential security solutions, this study aims to contribute to the development of effective strategies to bolster security measures in the rapidly evolving landscape of Big Data. The research will incorporate both primary research methods, such as surveys and interviews, and secondary research methods through an extensive literature review, to derive well-rounded and actionable insights.

**Comments and agreement from tutor**

Comments (Optional):

I confirm that the project is not work which has been or will be submitted for another qualification and is appropriate.

Agreed: (Name).....(Date).....

**Comments and agreement from project proposal checker (if applicable)**

Comments (Optional): Agreed:

(Name).....(Date).....

## 2. Ethical form.

### Section One: Basic details

**Project title:** Risks in computer system security and network security in Big Data Environments along with solutions to build better security systems

**Student name:** Tran Thanh Do

**Student number:** BH00124

**Programme:** Information technology.

**School:** British College BTEC-FPT

**Intended research start date:** 5-9-2023

**Intended research end date:** 15-12-2023

### Section Two: Project summary

Please select all research methods that you plan to use as part of your project:

- ☒ Interviews
- ☒ Questionnaires
- ☐ Observations
- ☐ Use of personal records
- ☒ Data analysis
- ☐ Action research
  
- ☐ Focus groups

Other (please specify): Primary research, Secondary research, Qualitative research, Quantitative research.

### Section Three: Participants

Please answer the following questions, giving full details where necessary.

Will your research involve human participants?

Who are the participants? Tick all that apply:

Children

How will participants be recruited (identified and approached)?

Describe the processes you will use to inform participants about what you are doing:

How will you obtain consent from participants? Will this be written? How will it be made clear to participants that they may withdraw consent to participate at any time?

**Studies involving questionnaires:**

Will participants be given the option of omitting questions they do not wish to answer?

☒ Yes

☐ No

If No please explain why below and ensure that you cover any ethical issues arising from this:

☒ Yes

☐ No

**Studies involving observation:**

Confirm whether participants will be asked for their informed consent to be observed.

Will you debrief participants at the end of their participation (i.e. give them a brief explanation of the study)?

☒ Yes

☐ No

Will participants be given information about the findings of your study? (This could be a brief summary of your findings in general.)

☐ Yes

☒ No

**Section Four: Data storage and security**

Confirm that all personal data will be stored and processed in compliance with the Data Protection Act (1998):

☒ Yes

☐ No

Who will have access to the data and personal information?

**During the research:**

Where will the data be stored?

Will mobile devices (such as USB storage and laptops) be used?

☒ Yes

☐ No

If yes, please provide further details: Laptop

**After the research:**

Where will the data be stored? My Laptop, One Drive, Google Drive

How long will the data and records be kept for and in what format?

Will data be kept for use by other researchers?

☒ Yes

☐ No

**Section Five: Ethical issues**

Are there any particular features of your proposed work which may raise ethical concerns?

☒ Yes

☐ No

If so, please outline how you will deal with these:

It is important that you demonstrate your awareness of potential risks that may arise as a result of your research. Please consider/address all issues that may apply. Ethical concerns may include, but are not limited to the following:

- Informed consent.
- Potentially vulnerable participants.
- Sensitive topics.
- Risks to participants and/or researchers.
- Confidentiality/anonymity.
- Disclosures/limits to confidentiality.
- Data storage and security, both during and after the research (including transfer, sharing, encryption, protection).
- Reporting.
- Dissemination and use of your findings.

### Section Six: Declaration

I have read, understood and will abide by *[insert centre name]* Research Ethics Policy:

☒ Yes

☐ No

I have discussed the ethical issues relating to my research with my Unit Tutor:

☒ Yes

☐ No

**I confirm that to the best of my knowledge:**

The above information is correct and that this is a full description of the ethics issues that may arise in the course of my research.

Name: Tran Thanh Do

Date: 10-10-2023

## H. CONCLUSION.

The article explores security risks in computer systems and networks within Big Data Environments. It highlights challenges such as scalability issues, data diversity, security vulnerabilities, and emphasizes proactive strategies to mitigate risks. Key measures include stringent access controls, robust encryption, advanced threat detection, and regulatory compliance. Proposed solutions encompass scalable distributed systems, efficient storage, and fostering a security-focused culture. Overall, the article underscores the vital need for a strategic approach to security in the rapidly expanding data landscape.

## I. REFERENCE.

- Primary vs Secondary Research – What’s the Difference? (2023) Qualtrics. Available at: <https://www.qualtrics.com/experience-management/research/primary-vs-secondary-research/> (Accessed: 10 October 2023).
- Streefkerk, R. (2023) Qualitative vs. Quantitative Research: Differences, Examples & Methods, Scribbr. Available at: <https://www.scribbr.com/methodology/qualitative-quantitative-research/> (Accessed: 10 October 2023).

- By, Mcleod, S., on, U. and 25, S. (2023) Qualitative vs Quantitative Research Methods & Data Analysis, Simply Psychology. Available at: <https://www.simplypsychology.org/qualitative-quantitative.html#:~:text=Quantitative%20research%20is%20often%20used> (Accessed: 10 October 2023).
- Kaspersky (2023) What is a firewall? Definition and explanation, www.kaspersky.com. Available at: <https://www.kaspersky.com/resource-center/definitions/firewall> (Accessed: 10 October 2023).
- Testing and validation: From hardware focus to full virtualization? (2017) McKinsey & Company. McKinsey & Company. Available at: <https://www.mckinsey.com/capabilities/operations/our-insights/testing-and-validation-from-hardware-focus-to-full-virtualization> (Accessed: 10 October 2023).