American Journal of Multidisciplinary Research & Development (AJMRD)
*Volume 06, Issue 02 (**February-2024**), PP 01-34*
ISSN: 2360-821X
www.ajmrd.com

Research Paper **Open Access**

Big Data Security Management in Digital Environment

Ehigiator Iyobor Egho-Promise[1], Mensah Sitti[2]

[1]*Dept of ICT, Faculty of CreaTech, City of Oxford College and University Centre, Oxford, UK*

[2]*Dept. of CSE, UMaT, Tarkwa Western Region, Ghana*

ABSTRACT:-

This study explores the complex subject of Big Data Security Management, focusing on the numerous opportunities and challenges presented by the contemporary data deluge. The research emphasises the importance of safeguarding data integrity and analytical configurations against a range of offline and online threats. Predicated on the research conducted by Manikandakumar and Ramanujam (2018). The imperative to address the escalating data security challenges across various industries—including healthcare, education, retail, and social networking—serves as the driving force behind this research. An International Business Machine (IBM) study accurately foretold that, as Jakóbik (2016) notes, in light of the ever-increasing data volumes, organisations must strengthen their security procedures more than ever before. The projected increase in the number of data scientists to 2.72 million, as stated by Shihab (2020), underscores the criticality of comprehending and executing strong security protocols. Due to the ever-changing nature of the internet, safeguarding private information and intellectual property is the principal focus of the research. Introducing novel data types into Hadoop pools generates fresh security challenges that necessitate customised resolutions. In order to resolve this knowledge vacuum, the present study examines the advantages and disadvantages of Big Data security, focusing on Hadoop systems, as well as potential mitigation strategies for organisations of different scales. The principal objective of this research is to identify and assess prospective remedies for safeguarding data throughout its complete life cycle, commencing with its collection and concluding with its processing. The study acknowledges the potential of Big Data, as described by Riaz et al. (2020), and emphasises the need for robust security protocols, even when managing enormous data sets. The literature review highlights the complexity of Big Data Security Management through the citation of scholarly works including Yuan (2017) and Moreno, Serrano, & Fernández-Medina (2016). It emphasises the importance of implementing strong security protocols in light of the growing reliance of organisations on big data for decision-making. Utilising questionnaire surveys and semi-structured interviews, the research strategy collects data from both subjective and objective sources in accordance with a mixed-methods approach. Priority is given to ensuring the safety, privacy, and anonymity of participants above all other considerations during the entirety of the research process. In essence, the primary objective of this study is to augment the ongoing discourse surrounding the management of security for big data by providing significant insights for academics, professionals, and policymakers. The study seeks to establish a secure digital environment for the continuously expanding data world by offering practical suggestions for organisations navigating the intricate terrain of Big Data security.

I. INTRODUCTION

1.1 Research Background

According to Demchenko et al. (2014), big Data Security encompasses all forms of defense to protect the data itself as well as protection against attacks, theft or other harmful activities that might interfere with a problem occurring in an analysis environment. All kinds of attacks--it can be compromised by online or offline attack. Data security management refers to making sure business information is safe and does not fall into unauthorized hands. Data security management systems stress the protection of sensitive data like private information or key proprietary resources for businesses. Take developing information security policies, identifying security risks and threats to IT systems as a few examples. Another key practice is disseminating information about data security best practices to employees across the organization, for example when opening email attachments (Jakóbik, 2016).

In the future data volumes will continue to increase. IMB conducted a study that forecasts there would be as many as 2.72 million data scientist workers available to help companies in dealing with all this information, and it turned out these estimates were correct. The greater use of big data would have a bearing on the way in which organizations understand and implement business intelligence and how it is protected. These days, no matter the field or technology Security is one of our major concerns. According to Manikandakumar& Ramanujam, (2018) compared to other areas that have securities issues and attacks occurring every single minute, these attacks are rather distinctive in a couple of ways. Firstly, the source data can be compromised as well; secondly it is possible for each version or component to vary from the others by some degree because sometimes there will not be attack vectors which allow modifications until they reach a specific threshold.

1.2 Research Problem

The research takes place within this vital area of Big Data Security Technology Management in the era of digitalization, while as data and analytics methods become increasingly important, so does securing them against possible threats (Moghadam, & Colomo-Palacios, 2018). As data volumes grow ever larger with each passing day, organizations are faced with the problem of how to deploy adequate security for sensitive information such as personal data and intellectual property. Because of the common practice in Big Data processing to amalgamate variety types of data into Hadoop pools, increasing their effect is another factor that makes implementation of strict security protocols even more significant. With so many sources and categories coming together in these lakes from all over the globe, other serious obstacles present themselves as well.

This research problem arises from the need to deal with security concerns amid increasing data usage. According to Moreno, Serrano & Fernández-Medina, (2016) in areas ranging from social networking to health care, retailing and education, the degree of digitization is so high that it threatens data security at every step in its lifecycle. It's essential therefore to pinpoint appropriate measures for preventing leakage or theft at each stage in this chain. The research seeks to understand how organizations, regardless of size, can negotiate the treacherous waters of Big Data security and particularly within a Hadoop environment. The all-important research question is how to find the best practice and tools to secure every aspect of data, from its collection through storage, analysis and processing (Riaz et al., 2020).

This research spans the many levels of data security in digital practice, recognising that problems can arise at any point when working with data. In this regard, the study will identify potential answers as well as best practices organizations can follow to protect themselves against security risks. Yet the research limitations are important because cybersecurity challenges and technologies they use are constantly evolving.

1.3 Research Aims and Objectives

The purpose of this research is to explore in depth and comprehensively the problems, dangers and data securities issues and possible security controls. To achieve this overarching goal, the following specific objectives have been identified:

- To assess the landscape of Big Data Security Management in the digital environment
- To examine the predicted expansion in data volumes, especially given Big Data's ever-growing use.
- To see how this growth affects organizations 'approaches to business intelligence and related security issues.
- To examine problems with data security when using Hadoop to process large sets of data.

1.4 Significance of the study

According to Salleh & Janczewski, (2016) recognizing its potential and its power, organizations are today increasingly adopting Big Data. Its most important feature is that data security takes priority. Due to this, many organizations now turn to Hadoop when processing large volumes of data. Whatever the size of organization, everyone works to save their data. These various kinds of data feed into the Hadoop process, in that they are gathered and stored in a Hadoop data lake where they are processed.A data management platform which comprises one or several Hadoop clusters to process and store nonrelational data is referred to as Hadoop data lake.

Given that it encompasses different kinds of data from multiple sources, strong security policies are necessary-all the more so since most companies handling Big Data work with sensitive information. According to Shihab, (2020) such sensitive data can range from credit card numbers to banking information, and even passwords. The importance of this data is not to be questioned, and it's more than just a matter of its size. To secure itself, an organization could turn to such techniques as installing firewalls to exclude the unauthorized and block intrusions; or establishing a reliable user authentication protocol--or rolling out thorough end-user training (Tang & Pan, 2015)

With data growing so rapidly in nearly every facet of human life, the issue of security has become especially important. According to Yuan, (2017) social networking sites, healthcare, retail and education are just some of the many different sectors in which social networks are huge. Digitization is everywhere, and security risks abound. The potential for a security breach is an issue that can arise anywhere in the process of data processing. Therefore, to raise this question and suggest its solution have been brought up at each level from accumulating data through storing it, analyzing it, or performing different operations on the information stored in memory. Therefore, steps that could secure the data had to be taken.

1.5 Research Question

The following is the research question developed by the researcher to conduct the study:

- How can organizations effectively manage and secure Big Data in the evolving digital landscape, considering the challenges posed by data growth, the impact on business intelligence, security challenges and the protection of sensitive information?

II. LITERATURE REVIEW

2.1 Overview of Data Security

Privacy, security, and trust are like three friends who always go hand in hand. They are connected similarly to how laws and ethics are related. When we talk about data privacy, we mean how information should be gathered, used, and accessed while respecting people's legal rights (Lee et al., 2016). On the ethical side, it is about our responsibilities, sometimes becoming duties we must fulfil (Knoppers & Thorogood, 2017). Nowadays, thanks to technology, a lot of research happens online. Researchers use methods like video calls for interviews, online surveys, analysing online conversations, studying web page content, checking discussion blogs, chat rooms, and emails, among other things (Cox, 2012). As time goes by, we see a lot of changes in society and technology. These changes affect how much and what kind of data researchers deal with (Fiesler, 2019). While the latest technology has many advantages, there are also some downsides. Sharing and storing data benefit researchers but also creates challenges, especially when keeping the data safe. In today's world, more than the old-fashioned ways we used to protect privacy and ensure security are needed to handle the explosion of data (Venkatraman & Venkatraman, 2019).

2.2 Importance of Data Security Management

Researchers deal with different data issues in their work, like changing existing data, keeping it safe, and sharing it. They must make ethical decisions in these situations (Boyd et al., 2016). Because of advanced technology, there is a growing risk of misusing data. Sticking to ethical standards is challenging (Hand, 2018). During their work, researchers also face various challenges related to data privacy. This includes ensuring computations are secure in distributed programming, safeguarding data storage and transaction logs, managing data origin, checking endpoints, and providing real-time secure monitoring (Mehta & Rao, 2015). The government and private institutions must create new software using the latest technology to tackle these issues. This software should protect data by maintaining privacy and preventing misuse, changes, and misinterpretation (etc.).

Nowadays, a lot of data has been created and it is becoming more important to handle it properly. People are developing different data management methods, and researchers are trying to find even better methods. One big aim is to keep the data safe. This can mean hiding some information, changing parts of it, or making it completely invisible to people who should not see it (D. R. Ingle et al., 2022). Data security means ensuring that only the right people can access it and nobody messes with it. This can be done using physical tools (like special hardware) and virtual tools (like specific software). One virtual method is data masking, where you change or hide the real information and replace it with something else to keep it safe from those who should not see it. Controlling who can see certain data is called Access Control. If this control is based on people's roles in a system, it is called role-based access control. Another way to protect data is through encryption, like turning readable information into unreadable. Many organisations use encryption to keep their data and their customers' data safe (D. R. Ingle et al., 2022).

2.3 Data Security Threats and Attacks

2.3.1 Cyber Threat Landscape:

The good things about computer technology are in trouble because of the increasing worries about internet crimes today. This is a big problem for the safety of the online world. Cybersecurity protects networks, computers, applications, and data from data disclosure, alteration and denial of data (Sutton, 2020). Cybersecurity experts discuss three main types of problems: malicious attacks, network attacks, and network abuse. A malicious attack is when someone or a malware causes harm to computer, network or data. Network attack is cybercrime that can cause harm such as Denial of Service (DoS), Session Hijacking, or Email Spoofing (Aboul-Enein, 2022). Network abuse is an attack against network traffic such as spam or phishing (Reiley and Rao, 2012).

People see cyber-attacks as crimes that happen over the internet. These can involve stealing a company's secrets, messing with online bank accounts, creating, and spreading viruses on different computers, putting private business info online, and even damaging a country's important national assets. Internet threats are seen as the biggest risk to businesses and can lead to a lot of money lost for organisations (Ponemon, 2012). Cyber threats are always changing, influenced by new technology, global tensions, and major events. Different players in this digital world, often called threat actors, use real-world changes to justify their actions (Kaloudi and Li, 2020). Over the past thirty years, cybersecurity threats have gotten smarter and more varied. This section talks about the current state of cybersecurity threats, explaining the main types and what makes them different. It also examines how security professionals can keep up by understanding the evolving threat landscape. Cyber threat actors vary greatly in their skills, tools, resources, and reasons for doing what they do (Chapple and Seidl, 2020). Some terms we might hear are "script kiddie," which is a nice way to describe someone who uses hacking tricks but is not skilled. Hacktivists use hacking for a cause they believe in. Insider attacks happen when someone with authorised access cause harm toorganization assets. For attackers to get into an organisation's systems, they usually need a way in, and email is a common method they exploit (Kaloudi and Li, 2020).

2.3.2 Insider Threats:

In today's digital world, strong cybersecurity is crucial for our economy. The biggest security threats come from inside, not outside. To deal with this, detecting and predicting these insider threats is important (Yazdinejad et al., 2023). Living in the digital age has its good and bad sides, just like anything else. The main problem is the security risk. Data breaches, where important information is exposed, are happening more often. Businesses, for example, face security risks from both inside and outside sources. Internal attacks, like from employees or vendors, are even riskier because these people have a direct connection and access to a company's computer system (Gheyas and Abdallah, 2016). Insiders know how the organisation works daily and have all the permissions needed to launch an attack that outsiders cannot do. The tricky part is that insiders can make their attacks look normal, making it hard to tell what they are up to (Hunker and Probst, 2021).

The current challenge revolves around implementing automated threat detection systems that balance effectiveness and avoid excessive false alarms. During time-sensitive situations, employees may encounter difficulties accessing the system, hindering their ability to perform critical tasks in emergencies. This predicament can incapacitate companies, leading to a loss of system availability, heightened expenses, diminished income, and tangible real-world risks. A noteworthy example underscores this concern when a whistleblower employee exposed 27,000 client records at Barclays Bank. The aftermath eroded customer trust and incurred £7.7 million in penalties, with an additional directive to pay affected parties up to £59 million in compensation. This incident represents just one in a series of occurrences arising from insider threats, emphasising the crucial need to explore preventive measures in today's context (Yazdinejad et al., 2022).

2.3.3 Advance Persistent Threat:

A super skilled and persistent enemy, known as Advance Persistent Adversary (APA), keeps improving at using advanced technology to carry out big cyber-attacks. One of the dangers they have encountered is called Advance Persistent Threat (APT), unlike regular cyber threats. This threat sticks to its goals for a long time, adapting to any attempts by defenders to catch it. It also keeps the connection between the host and server to take out its gathered data or cause damage to hardware when needed (Hussain, Ahmad and Uddin Ghouri, 2020). These APT attacks are special and complicated because they focus on a specific target compared to simpler attacks. The APA creates a kind of harmful software that aims to stay hidden for a long time, making APT tough to find and protect against (Chen, Desmet and Huygens, 2014). Usually, an APT attack goes through six steps, like a process.

- Information Gathering Step: The cyber adversaries first gather information about the organisation they want to target. They use technology and people to get as much information as possible about the organisation's network. This helps them find weak spots to sneak into the network. In this step, gathering information involves using technical methods and finding info from people who might not be very careful (Chen, Desmet and Huygens, 2014).
- Sneak In Step: In this step, the super-skilled adversary tries to get into the organisation's network using lots of different tricks. They use things like tricking people with fake emails (spear phishing), putting harmful code into the system using SQL injection, and taking advantage of weaknesses in the software system to find a way into the network (Chen, Desmet and Huygens, 2014).
- Keeping Access Step: Once the cyber adversaries enter the organisation's network, they use a remote administration tool (RAT) to keep their access and control. This tool talks to a command and control (C&C) server outside the organisation. The host and the external C&C server communication is usually encrypted

HTTP communication. This way, it can easily get past the network's firewall and defence systems by hiding itself to stay unnoticed (Chen, Desmet and Huygens, 2014).

- Moving Around Step: In this step, the APT malware moves from one part of the network to another on computers that are not infected yet. These other computers usually have more special access, making getting important information easier and having a better chance of taking out secret data (Chen, Desmet and Huygens, 2014).
- Taking Out Data Step: The last step in the APT cycle is taking out data. In this step, the host uploads the information collected to an external source or cloud. This can happen all at once or slowly without the person using the computer knowing about it (Chen, Desmet and Huygens, 2014).

2.4 Current Approaches to Data Security

2.4.1 Authentication and Encryption:

Authentication is figuring out who someone is when they want to use resources on the internet (Sun et al., 2019). There are four main ways to do this: (1) using a secret like a password; (2) having something like a key, either electronic or physical, that you own, which is often called a token; (3) using something that is part of you, like your fingerprint, face, or retina; and (4) doing something specific, like speaking or writing. Authentication also helps control who can get into a system by checking if the users' details match what is stored on the server. Biometric authentication, as discussed by Shah et al. (2015), plays a crucial role in both identifying and authenticating users within the realm of cloud data security. Biometrics can be categorised into two main classes: physiological and behavioural. Physiological biometrics pertain to variable characteristics unique to individuals and are associated with physical body parts, such as fingerprints and facial recognition. On the other hand, behavioural biometrics focuses on characteristics related to the behaviour of individuals, including signature and voice. Various features constitute biometric authentication technologies, encompassing fingerprint recognition, facial recognition, IRIS technology, hand geometry technology, retina geometry technology, speaker recognition, and signature verification techniques. As highlighted by Indu, Anand, and Bhaskar (2018) multifactor authentication involves the use of not just one but multiple factors for the verification of users. In the scenario of two-factor authentication, the combination of a username and password is used for identifying user during accessing cloud resources. Some additional factors, such as facial recognition, voice recognition, thumb impression, eye-ball scanner, and mobile identity number can be incorporated for enhancing the process of security authentication. Today, encryption is extensively used for protecting the information which is transmitted over the internet to make sure that the only designed/planned recipient can access the secure data. There are two main steps in the process of encryption, which include; conversion of plain text into cypher and enabling the receiver with a secret key for the decryption of the cypher text back into plain and readable text. In both these steps, for encryption and decryption, sender and receiver use a unique key. The difference between the types of encryptions depends on the number of keys that have been used which results in the creation of two main categories; symmetric encryption and asymmetric encryption (Sachdev and Bhansali, 2013).

Symmetric encryption, which is also known as single-key encryption depends on a single key for both encryption and decryption. To make sure the effectiveness of symmetric encryption there are two requirements that must be fulfilled. (1) a strong algorithm of encryption and (2) a safe transmission of secret key. The most well-known symmetric algorithms include 3DES, DES and the Advanced Encryption Standard (AES). Advanced encryption standard, specifically, is a very secure symmetric encryption algorithm exceeding the security levels of 3DES and DES. According to Stallings et al. (2020) AES has gained extensive use in major organisations due to its resistance against successful attacks. The organisations such as banks and government institutions mostly use AES. The second type is asymmetric encryption which is also called public-key encryption. According to Stallings et al. (2020) it involves two different keys: the secret key and the public key. RSA which is derived from the initial of its inventor's names (Rivest, Shamir and Adleman) is an extensively used algorithm for digital signatures and encryption (Mohsin et al., 2017). The security strength of this algorithm depends on the intricacy of calculating large numbers, and the private and public keys created by using two large prime numbers. Zhou and Tang (2011) have outlined that there are three steps in the RSA algorithm which include the generation of key, encryption and lastly decryption.

2.4.2 Access Control:

According to Mohamed et al. (2022) a fundamental part of data security has been formed by access control, that determines who is permitted to access specific resources and information within a system. The main objectives of access control include prevention of unauthorised access, disapproving exposure of data, and making sure that the compliance and regulations are being followed. There are different models of access control, some of them include mandatory access control (MAC), discretionary access control (DAC) and role-based access control (RBAC). Each model has its own unique strengths and limitations. According to Mohamed et al. (2022), for understanding the operation or process of access control, it is important to explore interrelated processes of authentication (confirmation of user identity) and authorisation (giving access on the basis of identity and policies). There are notable innovations and trends in the domain of access control. One such innovation is the principle of least privilege (PoLP) which focuses on the significance of providing users with a little access for performing their tasks. Another innovation or approach is attribute-based access control (ABAC) in which the attributes of user and properties of the resource are used for accessing decision. The advantages and challenges of implementing ABAC has been reported by Golightly et al. (2023), and it states policy complications and scalability. In challenging environments, the traditional methods of access control might fail with their continuous authentication (Colombo and Ferrari, 2019).

2.4.3 Security Policies and Procedures:

Ensuring information is safe depends on having strong rules and steps to keep it secure. Jorge, Pereira Da Silva, and Lopes Cardoso (2020) say that these rules make expectations clear, set the right way to behave, and create plans for dealing with important information. A security plan is like a big picture that shows the main ideas and goals for keeping data safe. It is a high-level document that explains why companies do certain security things. On the switch side, security steps turn the plan into very practical tasks by giving details on how should companies keep data safe. Steps further give specific instructions for situations like management of passwords or handling incidents (Jorge, Pereira Da Silva, and Lopes Cardoso, 2020).

Security policies and procedures are also essential for making sure the safety and integrity of information. The key components involve understanding the potential risks and vulnerabilities (Kuppusamy et al., 2020). This involves identification of possible threats and development of effective security measures for addressing them. Another critical aspect is classification of sensitivity-based data, enabling the hierarchization of security efforts and establishment of appropriate access controls. The Acceptable Use Policy (AUP) is also very crucial because it clarifies permitted and illegal activities when using organizational IT resources and data thus preventing the misuse and setting expectations for the user behaviour. Additionally, having an incident response plan is also vital for a well-defined approach in a security breach or data incident. Kuppusamy et al. (2020) emphasize that procedures should guide the identification, containment, eradication, and recovery during such incidents. It is worth noting that security policies and procedures are dynamic and should undergo regular review and updates to align with technological changes, regulations, and organizational needs (Angraini, Alias and Okfalisa, 2019).

2.4.4 Security Education and Training:

Security education, training, and awareness (SETA) programs keep reminding employees about important information security. These programs give employees crucial knowledge and skills. They help them understand why maintaining secure things is important and make them more aware of security issues (Hu, Hsu, and Zhou, 2021). SETA is a common, basic, and important strategy for ensuring organizations stay secure. Lots of organizations think of it as a top priority. For instance, the United States (US) Computer Security Act of 1987 says that every agency has to give regular training in computer security awareness and good computer practices to all employees (Al-Daeef, Basir, and Mohd, 2016). According to the US National Institute of Standards and Technology (NIST), not giving enough attention to security training is a big problem for a company. Managing the security of a company's resources involves technology and people (AlMindeel and Martins, 2020). Research shows that many security breaches and violations of information security rules happen because employees need to understand how important it is to secure information fully. This occurs when a company lacks Security Education, Training, and Awareness (SETA). A strong SETA program is important to ensure employees understand security issues and how to deal with security risks (AlMindeel and Martins, 2020). Many experts and professionals think companies should have SETA, but not many people who do it say their programs are "very effective" at making things more secure and changing how employees act. A lot of SETA programs could be better, and employees often do things that are not safe when it comes to computers (AlMindeel and Martins, 2020).

2.5 Challenges in Data Security Management

2.5.1 Rapidly Evolving Threat Landscapes:

For the businesses worldwide, it is important to protect electronic data from unauthorised access due to the persistent threats of cyber attackers, as they target corporate data and resources of information technology for their financial gain and also for geopolitical advantage (Saeed et al., 2023). Cybersecurity involves safeguarding individual or organisational electronic data; any attempt to gain unauthorised access is known as a cyber-attack. These attacks may include stealing private data, intellectual property, confidential business plans, or disrupting mission-critical IT systems. Organised crime syndicates and nation-state paramilitary cyber organisations now use cyber-attacks as operational strategies, leading to the emergence of Advanced Persistent Threats (APTs). Defending against these APTs is increasingly challenging for organisations, even with formalised cybersecurity systems (Kotsias, Ahmad, and Scheepers, 2022).

In recent years, there has been a significant increase in electronic attacks on the internet, and it is expected that new strategies will emerge. Cyber-attacks involve tactics individuals use to exploit weaknesses in electronic systems and networks, often to cause harm to systems or access sensitive information (Kotsias, Ahmad, and Scheepers, 2022). These attacks can originate from various sources, such as deceptive websites (unnatural links or fake) or malicious applications, and they are known to impact multiple industries (Aljanabi and Mijwil, 2023).

All electronic attacks seriously threaten the security of companies, institutions, and individuals. These attacks can result in the theft of data and information from devices. Additionally, they can disrupt services, business processes, and other aspects of the digital environment. Therefore, organisations must adopt practical tactics to address this issue and prevent it from negatively impacting their operations in the digital realm. Organisations rely on monitoring, detection, prevention, and response techniques as the most commonly used methods to thwart cyber-attacks. They continuously work to enhance these strategies, making them more effective in understanding the behaviour of electronic attacks. Cyberattacks refer to malicious activities targeting computer systems, networks, and devices on the internet to endanger or damage sensitive information (Illiashenko et al., 2023). Because of the valuable information computer systems contains, they specifically, are attractive to unauthorised individuals. Behind these attacks can be a single person, or a group of hackers that are motivated by political motives, personal reasons and financial gain. Mijwil et al. (2023) stated that it has been expected that the cost of cybercrime is predicted to exceeds $23 trillion by the year 2027 (Mijwil et al., 2023).

2.5.2 Compliance and Regulatory Issues:

In the fast-changing digital world, ensuring our data is secure is important. But dealing with all the rules and laws about it can take time and effort. This paragraph talks about the connection between data security, following the rules, and the laws there. It highlights the main problems, the best things to do, and the new trends in this area (Angraini, Alias, and Okfalisa, 2019). One big thing to get is compliance, which means sticking to the rules and laws that tell us how to protect data and privacy. Some examples are General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA), and Payment Card Industry Data Security Standard (PCI DSS) (Marotta and Madnick, 2020). Another super important part is data security, which means using different technical and admin tricks to keep data safe from people who shouldn't access or change it (Marotta and Madnick, 2020). This exploration wants to help us understand the challenges and changes happening in the digital world when it comes to keeping data safe and following the rules.

A big challenge is that there are many rules, and they sometimes overlap or disagree. This can be tough for companies working in different places because they must follow all the rules (Ali et al., 2021). If they don't follow the rules, there's a real risk of getting big fines, dealing with legal problems, and losing a good reputation. These consequences can hurt how much people trust a brand and how loyal customers are. Another big area for improvement is keeping up with new technology. The fast changes in things like cloud computing and the Internet of Things (IoT) bring new ways for malicious people to violate security rules. Changing how we keep data secure and following the rules to deal with these new threats (Li, Chen and Huang, 2021) are very important.

Small and Medium-sized Businesses (SMBs) have it tough because they sometimes need more money and experts to deal with all the complicated rules. This makes them more likely to break the rules and get into trouble (Ali et al., 2021). Altogether, these problems show how hard it is to balance keeping data safe, following the rules and dealing with the always-changing world of technology. Some new trends are shaping how we think about data security and following the rules. Privacy-enhancing Technologies (PETs) like homomorphic encryption and federated learning are cool solutions. They let us analyze data without showing the real data, which fits with what privacy rules want. Also, RegTech solutions help a lot by doing compliance tasks automatically and giving quick insights. This makes following the rules easier for organizations (Campbell, 2022).

One important thing is that countries are working together more on handling data. They're trying to make the rules about protecting data similar across borders. This makes it easier for global businesses to follow the rules without too much trouble (Campbell, 2022). So, it's not just a choice anymore for companies to follow data security rules; it's important for their success. Organizations can handle the rules better if they know the challenges, do the best things, and keep up with these new trends. This smart approach keeps important information safe and helps build trust with the people involved in a changing digital world.

2.5.3 Balancing Security and Usability

Balancing security and ease of use is a big challenge in keeping information safe (Di Nocera, Tempestini, and Orsini, 2023). It is important for the organisation to explore the right strategies for making a strong security without making things difficult for the users. Users can face some inconvenience, if the organisations top priority is security. The inconvenience can be in the form of strict rules about accessing data and complex sign-ins (Lennartsson et al., 2021).

However, if the focus of the organisation is more on making things convenient for users, leading to more restrictions and stronger passwords, makes it easy for the cyber attackers or unauthorized people to sign-in and create problems (Lennartsson et al., 2021). Managing the right balance is important. It is important for the organisations to specify how they can manage their security as well as make convenient access for the users. According to Alshamari (2016), it has been noted that there are important areas for making security and ease of use to work better. One area is unstable security principle which involves creation of secure and easy systems for people by involving easy way to access and remembers their logins and passwords (Alshamari, 2016). Another area is the human factor in security which involves exploring how people think and make their decisions. Additionally, teaching users about cybersecurity risks and staying safe online is another area which should be considered on top basis. This involves teaching and training users about different and possible cybersecurity risks, the best methods to be safe and common threats that can appear such as phishing scams. One of the most important things that companies can use is biometrics and the multifactor authentication. The main goal is to make the digital world more secure and safe by using new technologies and software as well as giving easy access to users (Damjan et al., 2023). There are some best practices to follow to find the right balance between security and ease of use. One important practice is the principle of least privilege which gives users the least access they need. This minimizes the potential damage if something goes wrong. Considering the context and risk is also very crucial. This means having stronger security for important data and situations while keeping things simpler for less important information and low-risk situations (Grobler, Gaire and Nepal, 2021). Using User-Centered Design is a must. It means designing security features with users in mind, including testing them to ensure they work well. Clear communication is also very important. Explaining security policies and procedures helps users understand why security measures are in place and encourages them to follow them (Hotz et al., 2022). However, there are still challenges and things to consider for the future. The constant evolution of threats and technologies requires continuous adaptation of security solutions and ongoing user education to maintain a balance. Balancing privacy with security remains a complex challenge, with technologies like encryption and anonymization offering potential solutions. Additionally, measuring the impact of security measures on both security and usability is crucial for informed decision-making and optimizing the delicate balance between these two essential aspects (Lapin and Šiurkus, 2022).

2.5.4 Insider Threat Mitigation:

Security threats can arise from within or outside an organisation, with insider attacks from employees, suppliers, or affiliated companies presenting a more insidious danger than external ones. Insiders possess intimate knowledge of an organisation's internal workings and hold all the necessary rights to execute an attack, making their actions appear like routine operations. Consequently, companies are allocating increased resources to defend against insider attacks in the coming years (Cooley, 2016). However, these protective measures could be rendered ineffective if not readily accessible when needed. The challenge lies in developing automated threat detection systems that strike a balance, avoiding excessive false alarms. A false security alert can lead to short-term or prolonged unavailability, hindering employees' access to the system during critical moments. This loss of availability can weaken a company, resulting in elevated costs, revenue loss, and reputational harm. The protection of systems and information hinges on fundamental aspects like availability, confidentiality, and integrity, with a breach in any of these constituting a security breach. To optimise these conflicting requirements, there is a need to create an Insider Threat Detection and Prediction Algorithm (IDPA) that minimises both false negatives and false positives (Gheyas and Abdallah, 2016).

III. RESEARCH METHODOLOGY

3.1 Research Philosophy

According to Davidavičienė, (2018) research philosophy is a set of beliefs, maxims, and presuppositions that govern the researcher's attitude to asking questions about reality. It is the starting point for research design, methodology and data analysis. As for research philosophy, one choice is as important because it influences how a researcher perceives reality, what he believes, knowledge to be, and the relationship between researchers themselves and their objects of study. In addition, there are three main research philosophies: positivism, interpretivism, and pragmatism.

As noted by Dźwigoł & Dźwigoł-Barosz, (2018) unlike reflexive realism, it strives to transcend, while interpretivism stresses objective understanding and conceptuality in contrast. Pragmatism sits in the middle, combining elements of both positivism and interpretivism with its focus on measurable outcomes achieved through flexible research methods. Once the research philosophy has been chosen, it guides a researcher in making methodological choices and interpreting findings; at last, the quality and credibility of his conclusions gradually take shape.

In the following study, the researcher used a pragmatic philosophy to conduct the study. The rationale for using this particular philosophy is that pragmatism recognizes all research topics and sees the value in using qualitative and quantitative methods to understand anything so complicated as human society. Eventually, only by using pragmatic philosophy in a mixed-method study can we get a full and practical picture with strong roots in this research question.

3.2 Research Approach

According to the study conducted by Snyder, (2019) a research approach means the overall framework or strategy for designing, coaching, and analyzing a survey. There are two main methods of research: deductive and inductive reasoning. The top-down deductive reasoning approach begins with a general theory or hypothesis and uses specific observations or experiments to test it. This method decides on predictions (or expectations) according to existing theories and uses real-life evidence to either confirm or refute these. In another study conducted by Opoku, Ahmed &Akotia, (2016) it was identified that qualitative research based on deductive reasoning is normally found in quantitative methods concerned with developing and testing hypotheses. The second type, inductive reasoning, proceeds from the particular to the universal. From specific observations or patterns of events, generalizations and theories are developed. This kind of inductive reasoning attempts to extrapolate general principles or theories from analyzing individual cases. It is frequently associated with qualitative research methods, which emphasize exploration and description to expose the latent meanings and patterns of a given setting.

In this study, the researcher has applied the deductive approach to complete the research process. The reasoned approach is justified because it is more hypothesis-driven and structured. Furthermore, the deductive method can also serve as a base point for three-point triangulation by linking quantifying results with qualitative views through such mechanisms as in-depth interviews and questionnaires. This combination adds depth to the research and broadens its scope. It provides a more comprehensive study of research problems.

3.3 Research Design

According to the study by Orngreen& Levinsen, (2017) research design allows researchers to systematically gather and analyze the data needed to answer research questions or test hypotheses. The qualitative research design focuses on exploration and in-depth understanding of complex phenomena. The approach is adaptable. Researchers can adjust the methodology while working through a study, and common techniques include interviews, focus groups, observations, and content analysis. However, quantitative research design is rigid and uses statistical tools to analyze numerical data according to a pre-determined plan, paying attention primarily to hypothesis testing.

As noted in Rajasekar &Verma, (2013) common quantitative research methods include surveys, experiments, and structured observations, which allow for discovering patterns and relationships. A mixed-methods research design integrates elements from qualitative and quantitative approaches, providing a more robust cover of the research problem. Thus, researchers use this method to avoid the limitations of using only one technique. The qualitative and quantitative data are collected sequentially or concurrently. The selection of research design depends on the nature and purpose of one’s data. Still, each approach allows the researcher to trace diverse angles in their influence on the studied phenomena.

In this study, the researcher has used a mixed-method design to collect the required research data. The justification for using mixed-method is that the iterative nature of mixed-methods research makes it possible for researchers to refine their questions and hypotheses based on initial quantitative data collection, thus producing much more focused and relevant results. This is especially helpful in answering questions better answered holistically based on depth and breadth.

3.4 Data Collection Method

According to the study conducted by Scheurich, (2014) data collection methods are the systematic procedures and techniques used to collect information or data relevant to researchers’ research objectives. These methods play a prominent role in the research design, and their selection is determined by factors such as the nature of the research question being asked; philosophy underlying the chosen methodology, and the overall aim of the study. Another study by Shirish, (2014) noted that collecting common research data includes questionnaires, interview observations, experiments, and analyzing documents. Surveys entail the presentation of pre-arranged questionnaires or questions designed to elicit answers from a sample of respondents, thus providing quantitative data. However, many interviews are structured, semi-structured, or unstructured; they explore the participants’ perspective and experiences more deeply than surveys.

Observation systematically observes and records events, behaviors, or phenomena in their natural settings. In experiments, variables are manipulated to examine cause and effect. To extract pertinent information, document analysis reviews written, visual, or audio materials, including texts, images, and recordings. Which data collection method to choose depends on what research question you are seeking an answer for, the aims of that part, and whether it's practical regarding resources and ethical considerations. Researchers often use a variety of methods, known as mixed-methods research. Choosing an appropriate data collection method is central to the validity and reliability of study results.

This study gathered information from primary sources using a questionnaire survey and semi-structured interviews. The survey involved 150 respondents. Also, the questionnaire was based on Google Forms, one of the most effective ways to send out a survey. Second, the questionnaire will be in Likert scale form with five options: strongly disagree, disagree, neutral opinion toward neither side opinion agrees, or strongly agree. Meanwhile, five informants were interviewed on a semi-structured basis—other than that, these respondents were recruited through Facebook and LinkedIn. In addition, the researcher also utilizes secondary data in the determinant of case studies or literature to compare a former researcher's work and report on relevant findings once this study's data collection is completed.

3.5 Data Analysis Method

Data analysis methods are the systematic procedures and means for inspecting, cleaning up (clean-up), transforming, and interpreting raw data to extract useful information to make informed decisions. Data properties, research questions and overall research design determine data analysis methods. These include descriptive statistics, inferential statistics (including regression analysis and the test of hypothesis), etc., all useful in quantitative research. Thematic analysis, content analysis, and grounded theory are techniques used in qualitative research to interrogate textual or visual data, looking for patterns, themes, and meanings. Mixed methods approaches, which combine quantitative and qualitative data analysis to understand complex phenomena better, have become increasingly common in recent years. Advanced technologies and software tools have also greatly impacted data analysis, enabling researchers to tackle large volumes of data, run complex analyses, and create beautiful graphics. However, no matter how the details are worked out, rigorous data analysis is necessary to ensure the validity and trustworthiness of the research findings.

The researcher in this study has analyzed the findings obtained by survey with SPSS software. The justification for using SPSS software is that SPSS makes it possible to manage and manipulate data quickly. Its spreadsheet-like format helps data organization, making it well-suited for exploratory data analysis. Besides powerful visualization tools, the software allows researchers to explain their findings through charts, graphs, and tables.

In addition, the researcher has applied thematic analysis to what is expressed through semi-structured interviews. The rationale for using thematic analysis is that its flexibility allows researchers to use the method on different forms of qualitative data, including interviews and written materials. A notable feature of thematic analysis is that it facilitates a coding and theme development process, which is simple even for novice researchers. Its ease and transparency make the entire procedure easily repeatable, thus raising inter-coder reliability. Furthermore, by its thematic approach and systematic rigor, thematic analysis is of irreplaceable value in explaining the intertwined realities behind human experience, behavior, and perception.

IV. DATA PROCESSING AND ANALYSIS

This chapter presents findings related to interviews and surveys that have been collected from respondents. After collecting data, data was cleaned and analysed in order to find the main key aspect related to subject matter of the study.

4.1 Data Collected

By employing a mixed-methods approach that combined qualitative and quantitative data collection techniques, the research questions were effectively investigated. A survey comprising 150 responses, which was conducted via Google Forms and employed a Likert scale, constituted a significant portion of the data. Using this technique, quantifiable opinions on the subjects were gathered. To acquire additional qualitative insights and a more comprehensive understanding of the research subject, semi-structured interviews were conducted with five informants. By incorporating secondary data obtained from case studies and literature, the conclusions drawn could be further elucidated and situated within the context of previous research.

4.2 Processing of Data

Data Processing: Sensitive processing was employed to guarantee the precision and dependability of the gathered data. Visualisation tools and statistical methods, including inferential and descriptive statistics, were employed to analyse the quantitative data obtained from the survey questionnaire in SPSS. Thematic analysis was employed to extract significant patterns and insights from the data obtained from the semi-structured interviews. Adoption of theme analysis was prompted by its adaptability, usability, and efficacy in extracting meaning from qualitative data.

4.3 Interpretation

The objective of the data interpretation phase was to formulate conclusions regarding the research questions based on the examined data. We examined the survey questions for trends, patterns, and statistical significance as part of the process of analysing quantitative data. Thematic analysis was employed to interpret qualitative data, revealing recurring patterns and themes within the narratives provided by the participants. An in-depth comprehension of the subject matter was enhanced through the process of comparison analyses with secondary data, which served to validate and contextualise the research findings.

4.4 Thematic Analysis

Toanalyse, interview data, thematic analysis have been used. After analysing the transcripts, the following themes were generated that are in line with the main objective of the study. This analytical effort aims to comprehend the complicated network of participant responses to key interview questions, each of which is designed to illuminate a certain facet of data security. The study examines the challenges businesses face in managing large data security. In the digital environment, when data volumes expand, the security vulnerabilities increase also and effective security mechanisms are essential. Participants' perspectives may illuminate data proliferation's pros and cons and the effective security solutions are required to manage it. Due to exponential data expansion, data protection and management have evolved. This essay highlights the need for evaluation, security modification, and business intelligence activities and explains Hadoop installation challenges on large datasets. We assess Hadoop's weaknesses, vulnerabilities, and data security impact to provide readers a complete picture. Scalability, prevention, and best practices are essential for Big Data security. Organisational implementation of data protection legislation. This inquiry covers privacy, governance, and adherence issues, new technologies, machine learning, and Artificial Intelligence (AI) may improve security of assets. A strong strategy, scalable security technologies, and sophisticated analytics are needed to identify oncoming threats.

4.4.1 Current Landscape of Big Data Security Management

Big Data Security Management is an interdisciplinary field that utilizes an extensive range of approaches, methodologies, and frameworks to confront the obstacles presented by the swiftly evolving big data sector. Ensuring data security has become an increasingly formidable task in recent years due to the exponential expansion of data in the digital realm (Bibri, 2018). This sudden increase in data volume has highlighted the necessity for comprehensive security measures throughout the entire data lifecycle, including collection, storage, analysis, and processing. Respondent 2 correctly highlighted the need of Big Data Security Management in addressing data complexity, which affects trust and reputation. Respondent 7 emphasises the importance of security policies in safeguarding firm digital assets and facilitating safe digital transformation. This shows Big Data's vulnerability to attackers.

Presently, the sector is preoccupied with the difficulty of comprehending the intricacies of large data security management. Organizations are confronted with diverse data types that originate from numerous locations and exist in multiple formats. The complexity of security measures necessitates a nuanced approach, given that distinct data types may require varying degrees of safeguarding. Instances of data categories that necessitate more stringent controls include non-sensitive, non-personal data, and sensitive personal information. According to respondent 1 Big Data Security Management is crucial to tackling data concerns from commercial apps, IoT devices, and social media platforms. Respondent 5 emphasises the difficulty of safely enabling innovation in diverse ecosystems such as cloud-based solutions, Hadoop, Spark, and NoSQL databases which highlights its importance. Respondent 6 further stresses the need of Big Data Security Management in ensuring GDPR and HIPAA compliance to avoid financial and legal penalties. Both parties accept the constant growth of the digital world and emphasise the need of proactive security systems to react to new hazards

4.4.2 Impact of Predicted Expansion in Data Volumes

Valacich and Schneider (2018) argue that the significant expansion of data volumes resulting from the growing digitization of numerous businesses gives rise to various prospects and obstacles concerning data security. An enduring obstacle in evaluating its effects is the projected surge in data volume and the accompanying complexities. Considering the exponential growth of data, organizations ought to reassess their security protocols.

Respondent 8 observed that data quantities are increasing the need for proactive data protection. Since more data means more vulnerabilities, yes. Respondent 10 highlights numerous important issues, including data mining and analytics that preserve privacy, unsecure data transport and storage, and endpoint input validation. These technologies facilitate the ability of organizations to adapt to the constantly changing landscape of cyber threats by enabling a proactive approach to security rather than a reactive one. It continues to emphasize that adaptable security measures are required to accommodate the anticipated increase in data volumes (Sivarajah et al., 2017).

As stated by Respondent 1, institutions are tasked with the management and protection of an extensive variety of data sources, formats, and types because of the exponential growth of data volumes. Respondent 6 reiterates the importance of robust privacy protections and rigorous adherence to regulations considering the increasing proliferation of privacy issues resulting from this expansion. Respondent 8, acknowledging the potential negative ramifications of insufficient protocols regarding big data security management, emphasises the criticality of implementing proactive measures and infrastructure to efficiently manage the expanding volume of data.

4.4.3 Influence on Organizations' Approaches to Business Intelligence

Organizations are compelled to reassess conventional approaches and tactically modify security strategies in light of the exponential expansion of data volumes, which significantly impacts business intelligence. Organizations, specifically those engaged in business intelligence operations, must reconsider their data administration and security approaches, considering the enormous volumes of data produced during the digital age (Grover et al., 2018). Critical subjects encompass the imperative to reassess conventional approaches in light of the exponential growth of data volumes. Respondent 7 stressed the need to manage data access and user rights in Business Intelligence (BI) systems as data grows. Secure authorization and authentication mechanisms must be used to restrict access to datasets and insights to protect sensitive data. However, respondent 10 underlines that massive data sets may provide firms real-time information to make better, customer-centric choices.

Furthermore, business intelligence processes experience significant disruptions. The profusion and variety of data readily accessible to an organization may facilitate the generation of more profound insights and formulating more informed decisions (Hossain et al., 2019). Nonetheless, to accomplish this, accessibility and security must be meticulously balanced. Organizations should implement business intelligence processes to ensure the security of sensitive information and derive value from large datasets (Karafiloski&Mishev, 2017).

According to Respondent 1, data volume forces companies to employ scalable Business Intelligence (BI) solutions. Respondent 5 said that cloud-based BI solutions also help BI platforms flourish. Respondent 6 highlights the necessity for encryption and multi-factor authentication for BI platforms to address rising security issues. Respondent 8 adds that data quantities provide firms an edge in the shifting commercial world. This improves decision-making and business intelligence.

4.4.4 Security Challenges with Hadoop

There are benefits and drawbacks in utilizing Hadoop to analyze vast quantities of data; specifically, one should be aware of this technology's security risks. A recurring motif is directing focus toward the prevalent challenges and susceptibilities linked to Hadoop, disclosing its deficiencies in design, and investigating possible remedies for these issues. A prominent concern is the Hadoop vulnerabilities that could potentially result in security intrusions for organizations (Manogaran et al., 2017). Hadoop functions as a decentralized database management system that leverages cost-effective hardware clusters to store and process enormous volumes of data. Data governance, encryption, and access control issues manifest due to the distributed architecture of Hadoop. Respondent 2, 5 and 6, data encryption, job and resource management security and audit and Logging are major challenges. Insufficient audit and logging capabilities make it challenging to monitor and trace activities within the Hadoop cluster. Without comprehensive auditing, it becomes difficult to investigate security incidents or track user actions, potentially delaying the detection of unauthorized activities.

4.4.5 Integrating Security Measures into Big Data Infrastructure

Incorporating security measures into big data infrastructure is imperative for organizations to optimize the advantages of big data processing while mitigating associated risks. This subject examines the difficulties associated with smoothly integrating security into the infrastructure. It also emphasizes implementing proactive security measures, following integration best practices, and ensuring scalability. Infrastructure for Big Data must be scalable, which is a significant concern (Mooney and Pejaver, 2018). Organizations must be able to effectively handle escalating burdens and processing requirements due to the perpetual growth of the datasets they handle. Security mechanisms also consider scalability in conjunction with data processing. Integration of effective security solutions must increase in tandem with the volume of data as the infrastructure grows; otherwise, security measures will only be able to match the complexity of potential threats. Additionally vital is the subject of integration of best practices.

Respondent 6 recommended advanced data privacy and security solutions including anonymization and obfuscation. This may be used with Respondent 7's advice of real-time monitoring and recording to protect sensitive data in data sharing for analytics or cooperation with other organisations. This includes monitoring user activities, spotting abnormalities, and reacting quickly to threats and vulnerabilities.

Organizations can reduce the likelihood of data breaches and unauthorized access by integrating security as a fundamental element into their Big Data architecture and promptly addressing any security concerns (N. et al., 2022). Integrating security into Big Data infrastructure is a complex procedure that includes defining the significance of proactive security measures, incorporating best practices, adopting Secured by Design (SBD) principles and addressing scalability requirements. According to respondent 8 and 10, network security requires a thorough plan. Scalability issues may be addressed by implementing data encryption, secure data transfer, and server and database access constraints. Network security solutions should include data backup and recovery, strong data storage architecture, risk assessments, security compliance automation, and team communication.

4.4.6 Compliance with Data Security Regulations

Constraints regarding data security regulations are more critical than ever for organizations operating in the Big Data industry, given the constant evolution of privacy laws. Privacy concerns arising from managing sensitive information, the difficulties organizations encounter in adhering to regulatory requirements, and the pivotal significance of governance frameworks in attaining and sustaining conformance are among the numerous topics addressed in this extensive field of study (Pappas et al., 2018). The difficulties businesses face in adhering to data security regulations are one of the main aspects. New rules and regulations are frequently implemented in response to the dynamic nature of the regulatory environment and the demands of emergent technologies and hazards.

Respondents 1 and 5 declared AI is revolutionising cyber security with behavioral analysis, automated response and remediation, better authentication, predictive analysis, and anomaly detection. AI outsources threat detection, surpassing software-driven alternatives. This allows proactive defenses against emerging assaults and ensures security and resilience.

ML algorithms can predict potential security threats based on historical data and current trends. This enables organizations to anticipate and prevent security incidents before they occur, providing a proactive security posture.

4.5 Analysis of Survey Dataset

In this section, survey data was analyzed using Statistical Package for Social Science (SPSS). Frequency distribution has been used to find the preferences and responses of the respondents related to survey questions. Table 1 shows brief information on the demographic of respondents who participated in the survey.

Table 1: Gender of Respondents

	Frequency	(%)
Male	17	68
Female	8	32
Total	25	100
Age Group of Respondents		
18-25	2	8
26-35	3	12
36-45	14	56
46-55	6	24
Above 55	0	0
Total	25	100
Educational background		
High School	2	8
Bachelor	3	12
Masters	4	16
Above Masters	16	64
Total	25	100
Working experience as a Data Security Management		
3 to 5	6	24
6 to 10	2	8
11 to 15	4	16
Above 15 years	13	52
Total	25	100

Figure 1: Gender of Respondents

It has been found that 68 percent of respondents are male whereas; 32 percent of respondents are female. As per age group, it can be seen that 56 percent respondents belong to age group of 36 to 45, 24 percent of respondents belong to age group of 46 to 55, 12 percent respondents belong to age group of 26 to 35 and only 8 percent of respondents belongs to age group of 18 to 25 and finally 0 percent of respondents belongs to age group above 55. In terms of their educational background, 64 percent of respondents have above master's level degrees, 16 percent respondents have master's degree, 12 percent respondents have bachelor degree and only 8 percent respondents have high school level degree. Lastly, in terms of working experience as a data security management 52 percent respondents have above 15 years of working experience, 16 percent respondents have 11 to 15 years of working experience. 24 percent of respondent have 3 to 5 years of working experience.

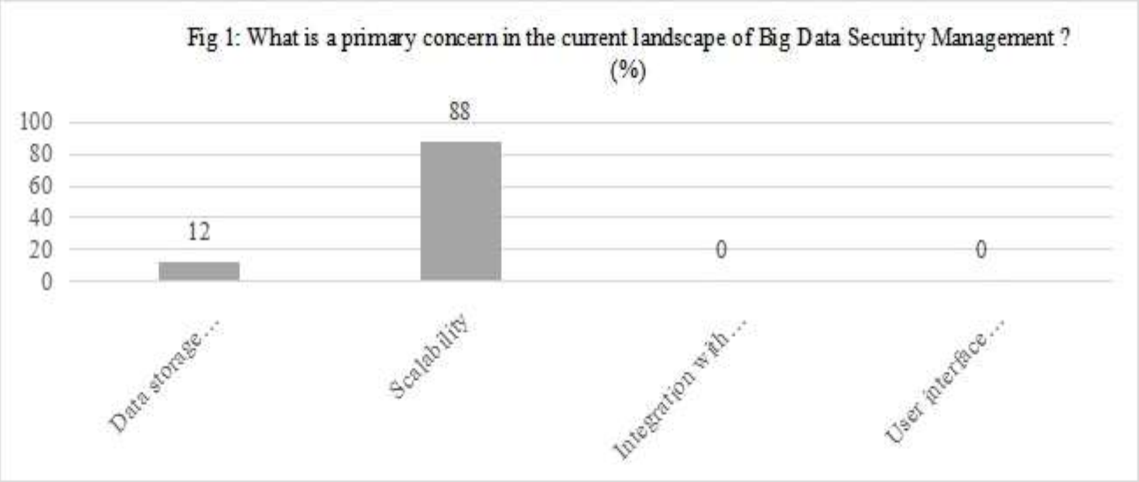

Figure 2: What is a primary concern in the current landscape of Big Data Security Management?

Respondents were asked questions about primary concerns in the current big data security management landscape. 88 percent of respondents think scalability is the primary concern, whereas 12 percent believe data storage efficiency is a primary concern in the current landscape. No respondent considered integration with IOT devices and user interface design the primary concern.

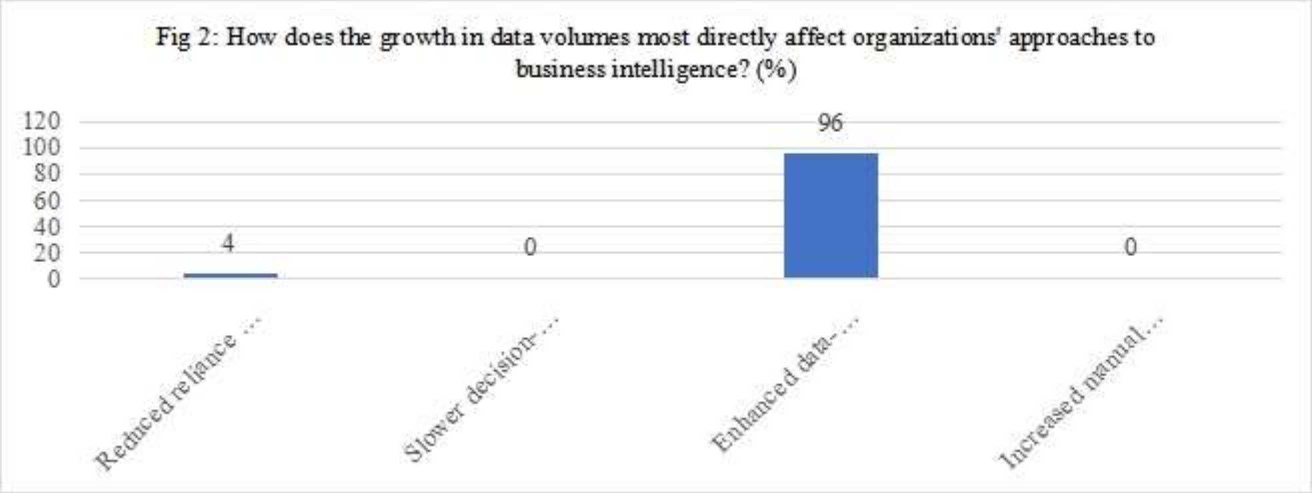

Figure 3:How might the predicted expansion in data volumes impact Big Data Security Management

Questions related to data volume growth most directly affecting organizations' approaches to business intelligence were asked. 96 percent of respondents think that enhanced data-driven decision-making is the main aspect of data volume growth that directly affects organizational approaches to business intelligence. Only 4 percent of respondents believe reduced reliance on data analytics can also be an aspect of growth. The growth in data volumes most directly affects organizations' approaches to business intelligence. None of the respondents think that slower decision-making processes and increased manual data processes can be the main factors of growth in data volumes that most directly affect organizations' approaches to business intelligence.

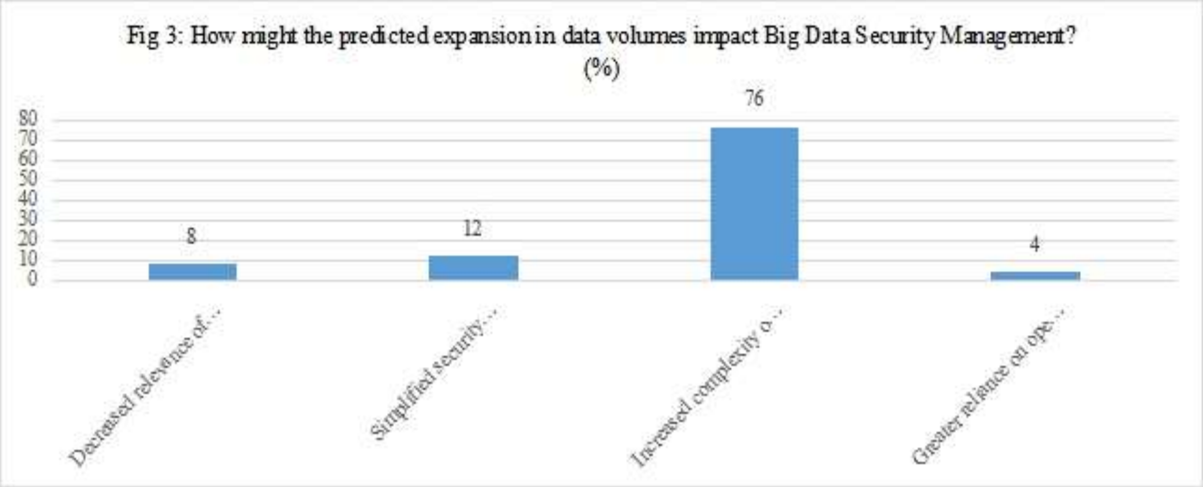

Figure 4: How does the growth in data volumes most directly affect organizations' approaches to business intelligence?

Questions related to “How might the predicted expansion in data volumes impact Big Data Security Management?” were asked by respondents. It has been found that predicted expansion through increased complexity of security challenges in data volume can impact big data security management, according to 76 percent of respondents. Furthermore, 12 percent of respondents think that simplified security protocols for predicted expansion in data volume may impact big data security management, 8 percent of respondents think that decreased relevance of security measures, and 4 percent of respondents consider greater reliance on open-source security tools are the major aspects of predicted expansion in data volumes impact big data security management.

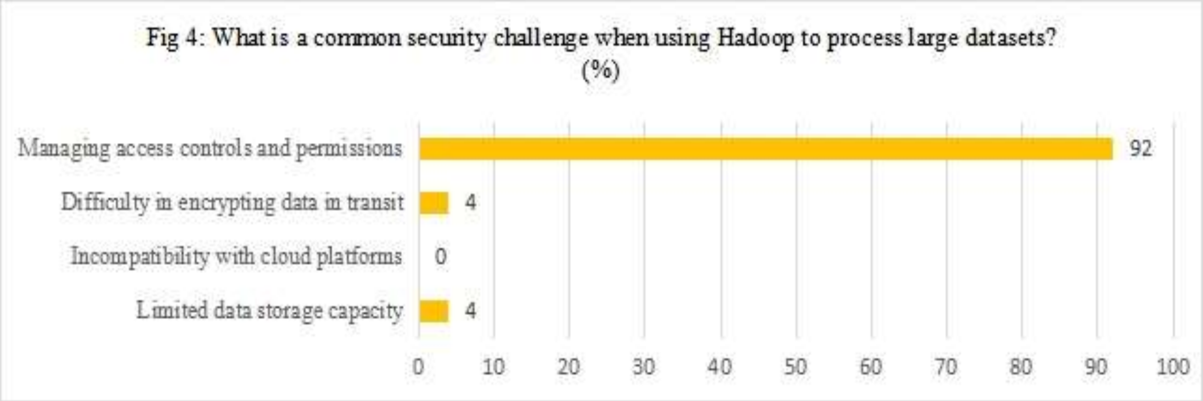

Figure 5: What is a common security challenge when using Hadoop to process large datasets?

Findings show that managing access control and permission is a common security challenge when using Hadoop to process large datasets, according to 92 percent of respondents. Furthermore, 8 percent of respondents think that difficulty encrypting data in transit and limited data storage capacity are common security challenges when using Hadoop to process large datasets. None of the respondents considered incompatibility with cloud platforms a common security challenge when using Hadoop to process large datasets.

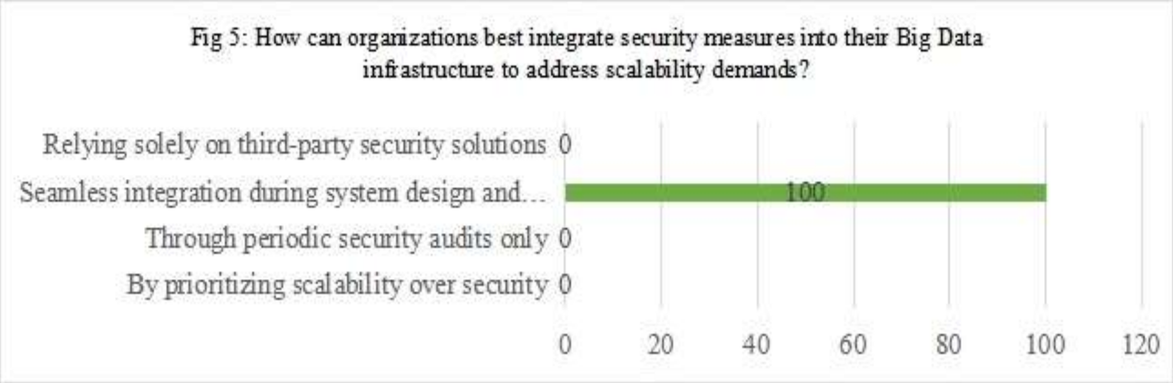

Figure 6: How can organizations best integrate security measures into their Big Data infrastructure to address scalability demands?

Through seamless integration during system design and implementation, organizations can best integrate security measures into their Big Data infrastructure to address scalability demands.

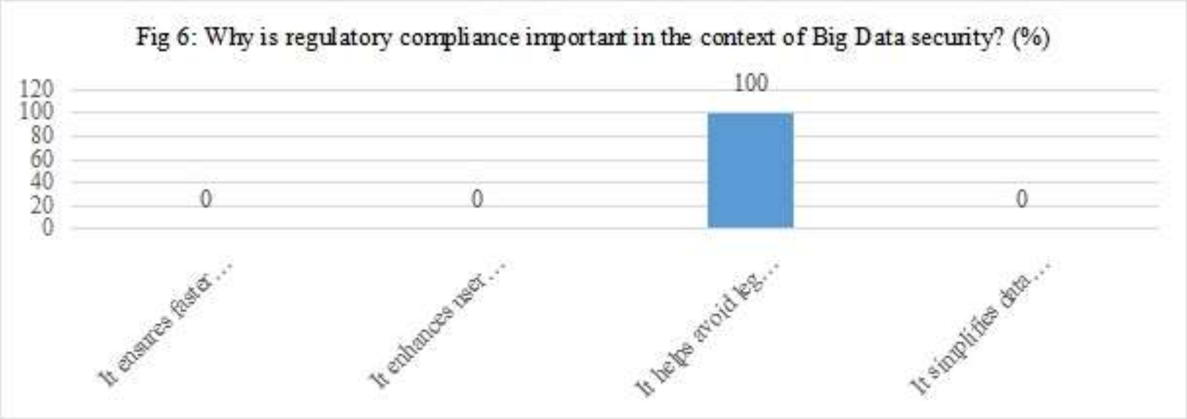

Figure 7:Why is regulatory compliance important in the context of Big Data security?

All respondents think regulatory compliance is important in the context of Big Data security because It helps avoid legal consequences and fines.

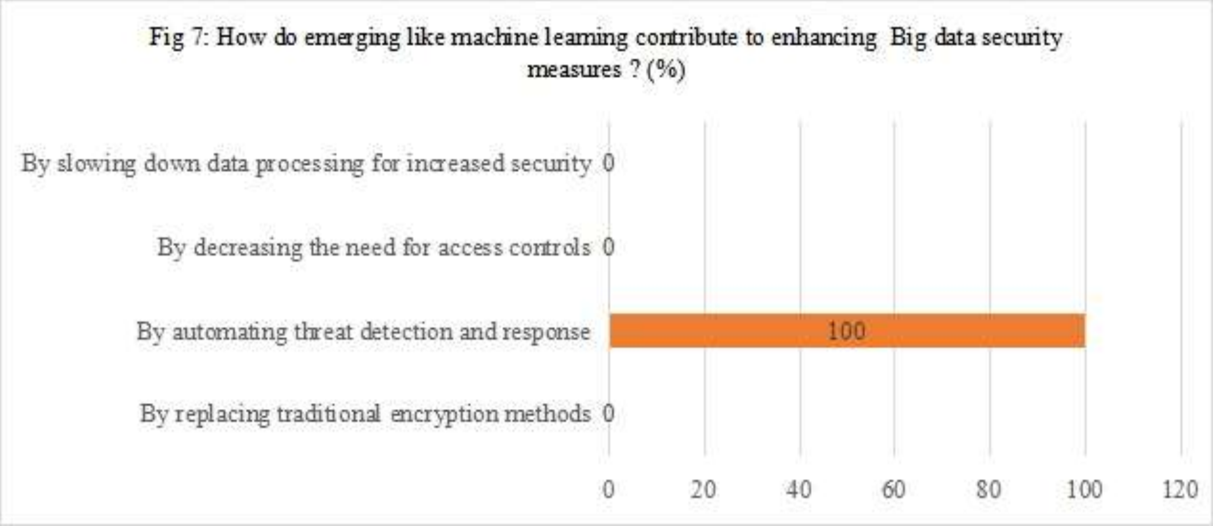

Figure 8: How do emerging technologies like machine learning contribute to enhancing Big Data security measures?

All respondents pointed out that by automating threat detection and response, emerging technologies like machine learning contribute to enhancing Big data security measures.

V. CONCLUSION

5.1 Conclusion

This study explores the critical domain of big data security management in the digital environment. It highlights the manifold prospects and obstacles presented by the exponential expansion of data. Manikandakumar and Ramanujam (2018) posit that the domain of big data security encompasses a multitude of attack vectors. In light of the increasing workforce of data scientists and the escalating volume of data (as demonstrated by an IBM study and supported by subsequent occurrences), organizations must strengthen their security protocols beyond reasonable doubt (Shihab, 2020). The proliferation of digital technologies across various industries—including education, healthcare, social media, and retail—has heightened the significance of data security issues, thereby motivating the investigation at hand. Since digital activities are involved in each phase of the data lifecycle, safeguards against loss or disclosure must be meticulously considered. The investigation of the present condition of Big Data Security Management, the ramifications for the business intelligence endeavors of organizations, and the escalation in data volumes are fundamental elements of the research's particular objectives. In order to acquire data for the subsequent phase, scholars will employ a mixed-method research approach, which integrates semi-structured interviews and questionnaire surveys. Using the selected methodology, we can examine the security of big data from all subjective and objective perspectives. The survey was structured to encompass a sample size of 150 individuals. Furthermore, it incorporated five interviews with informants and SPSS wasused for data analyses.

In order to shed light on the myriad prospects and obstacles arising from the exponential expansion of data volumes, this research concludes that the investigation and security of big data in the digital environment is imperative. This study examines the concerns regarding the security of Big Data that organization of various scales encounter, concentrating on the Hadoop ecosystem. Its inception was motivated by the urgent need to address the escalating anxieties surrounding data security. How to identify the most efficient resources and strategies for protecting data throughout its entire lifecycle—from acquisition to storage, analysis, and processing—is the primary focus of research. This research underscores the importance of comprehending and executing resilient security protocols amidst perpetually changing technological digital environments. The significance of this research is paramount, given the increasing relevance of Big Data across various industries, as noted by Riaz et al. (2020). In an era where even, the smallest businesses vie for Hadoop's processing power and data lake storage space, implementing stringent security measures is more important than ever. According to the study, it is a prevalent aspect of contemporary data processing to manage enormous quantities of sensitive data, including intellectual property and personal information. Therefore, ensuring the security of this information is of the utmost importance. It necessitates a holistic approach that considers the numerous data sources, formats, and varieties in addition to quantity. To ensure that security initiatives align with overarching corporate objectives, a comprehensive approach that considers organizational culture and governance structures is emphasized in the study.

REFERENCES

[1]. Abels, E., Pantanowitz, L., Aeffner, F., Zarella, M. D., van der Laak, J., Bui, M. M., ... & Kozlowski, C. (2019). Computational pathology definitions, best practices, and recommendations for regulatory guidance: a white paper from the Digital Pathology Association. The Journal of pathology, 249(3), 286-294.https://doi.org/10.1002/path.5331

[2]. Aboul-Enein, S. (2022). Cybersecurity Challenges in the Middle East. [online] Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/GCSP-Cybersecurity%20Challenges%20in%20the%20Middle%20East.pdf.

[3]. Aivazpour, Z., Valecha, R., & Chakraborty, R. (2022). Data breaches: An empirical study of the effect of monitoring services. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 53(4), 65-82.(https://dl.acm.org/doi/abs/10.1145/3571823.3571829).

[4]. Al Sabbagh, B. (2019). Cybersecurity Incident Response A Socio-Technical Approach. [online] Available at: https://www.diva-portal.org/smash/get/diva2:1303567/FULLTEXT01.pdf.

[5]. Al-Daeef, M.M., Basir, N. & Mohd, M. (2016). Security Awareness Training: A Review. [online] Semantic Scholar. Available at: https://www.semanticscholar.org/paper/Security-Awareness-Training%3A-A-Review-Al-Daeef-Basir/f040209717c34624dcb97ccd3ca8acc2e0d8ed93.

[6]. Ali, R.F., Dominic, P.D.D., Ali, S.E.A., Rehman, M. & Sohail, A. (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. Applied Sciences, 11(8), p.3383. doi:https://doi.org/10.3390/app11083383.

[7]. Aljanabi, M. &Mijwil, M.M. (2023). ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information. Mesopotamian Journal of CyberSecurity. [online] Available at:

https://www.academia.edu/96642258/ChatGPT_Exploring_the_Role_of_Cybersecurity_in_the_Protection_of_Medical_Information [Accessed 19 Dec. 2023].

[8]. AlMindeel, R. & Martins, J.T. (2020). Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. Information Technology & People, ahead-of-print(ahead-of-print). doi:https://doi.org/10.1108/itp-06-2019-0269.

[9]. Alshamari, M. (2016). A Review of Gaps between Usability and Security/Privacy. International Journal of Communications, Network and System Sciences, [online] 09(10), pp.413–429. doi:https://doi.org/10.4236/ijcns.2016.910034.

[10]. Alturi, V. & Ferraiolo, D. (2011). Role-Based Access Control. Encyclopedia of Cryptography and Security, pp.1053–1055. doi:https://doi.org/10.1007/978-1-4419-5906-5_829.

[11]. Alyousif, N. & Sultan Alhabis (2022). The Necessity of Multi Factor Authentication. International Journal of Computer Science and Information Technology Research, 10(2). doi:https://doi.org/10.5281/zenodo.6472757.

[12]. Angraini, Alias, R.A. &Okfalisa (2019). Information Security Policy Compliance: Systematic Literature Review. Procedia Computer Science, 161, pp.1216–1224. doi:https://doi.org/10.1016/j.procs.2019.11.235.

[13]. Ashraf, M. (2022). The role of peer events in corporate governance: Evidence from data breaches. The Accounting Review, 97(2), 1-24. https://doi.org/10.2308/TAR-2019-1033

[14]. Bakhsh, S.T., Alghamdi, S., Alsemmeari, R.A. & Hassan, S.R. (2019). An adaptive intrusion detection and prevention system for Internet of Things. International Journal of Distributed Sensor Networks, 15(11), p.155014771988810. doi:https://doi.org/10.1177/1550147719888109.

[15]. Campbell, C. (2022). CUNY Academic Works CUNY Academic Works A Review of Data Protection Regulations and the Right to Privacy: A Review of Data Protection Regulations and the Right to Privacy: the case of the US and India the case of the US and India. [online] Available at: https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=2024&context=cc_etds_theses.

[16]. Chapple, M. & Seidl, D. (2020). Cybersecurity Threat Landscape | part of CompTIA Security+ Study Guide: Exam SY0-601 | Wiley Data and Cybersecurity books | IEEE Xplore. [online] ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/9936725 [Accessed 19 Dec. 2023].

[17]. Chase, J. (2014). JPMorgan Chase & Co. Annual Report 2014. (https://www.rns-pdf.londonstockexchange.com/rns/5271A_1-2014-12-22.pdf).

[18]. Chen, P., Desmet, L. & Huygens, C. (2014). A Study on Advanced Persistent Threats. Advanced Information Systems Engineering, 8735, pp.63–72. doi:https://doi.org/10.1007/978-3-662-44885-4_5.

[19]. Choi, Y.-H., Liu, P., Shang, Z., Wang, H., Wang, Z., Zhang, L., Zhou, J. & Zou, Q. (2020). Using deep learning to solve computer security challenges: a survey. Cybersecurity, 3(1). doi:https://doi.org/10.1186/s42400-020-00055-5.

[20]. Colombo, P. & Ferrari, E. (2019). Access control technologies for Big Data management systems: literature review and future trends. Cybersecurity, 2(1). doi:https://doi.org/10.1186/s42400-018-0020-9.

[21]. Cooley, G. (2016). Insider Threats' Behaviors and Data Security Management Insider Threats' Behaviors and Data Security Management Strategies Strategies. [online] Available at: https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=12251&context=dissertations.

[22]. Cooley, G. (2016). Insider Threats' Behaviors and Data Security Management Insider Threats' Behaviors and Data Security Management Strategies Strategies. [online] Available at: https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=12251&context=dissertations.

[23]. D. R. Ingle, Dr., Kulkarni, M., Shinde, P. & Tambe, M. (2022). Literature Review of Data Security Measures and Access Control Mechanisms of Information Security. International Journal of Creative Research Thoughts, 10(4).

[24]. Damjan Fujs, Vrhovec, S. & Damjan Vavpotič (2023). Balancing software and training requirements for information security. Computers & Security, 134, pp.103467–103467. doi:https://doi.org/10.1016/j.cose.2023.103467.

[25]. Davidavičienė, V., (2018). Research methodology: An introduction. Modernising the Academic Teaching and Research Environment: Methodologies and Cases in Business Research, pp.1-23.

[26]. Demchenko, Y., Ngo, C., de Laat, C., Membrey, P. &Gordijenko, D., (2014). Big security for big data: Addressing security challenges for the big data infrastructure. In Secure Data Management: 10th VLDB Workshop, SDM 2013, Trento, Italy, August 30, 2013, Proceedings 10 (pp. 76-94). Springer International Publishing.

[27]. Denning, D.E. (1987). An Intrusion-Detection Model. IEEE Transactions on Software Engineering, [online] SE-13(2), pp.222–232. doi:https://doi.org/10.1109/TSE.1987.232894.

[28]. Di Nocera, F., Tempestini, G. & Orsini, M. (2023). Usable Security: A Systematic Literature Review. Information, [online] 14(12), p.641. doi:https://doi.org/10.3390/info14120641.

[29]. Duncan, B. & Whittington, M. (2016). Cloud Cyber-Security: Empowering the Audit Trail. International Journal on Advances in Security, [online] 9. Available at: http://personales.upv.es/thinkmind/dl/journals/sec/sec_v9_n34_2016/sec_v9_n34_2016_8.pdf [Accessed 21 Dec. 2023].

[30]. Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., & Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. International journal of information management, 55, 102211.https://doi.org/10.1016/j.ijinfomgt.2020.102211

[31]. Dźwigoł, H. &Dźwigoł-Barosz, M., (2018). Scientific research methodology in management sciences. Financial and credit activity problems of theory and practice, 2(25), pp.424-437.

[32]. Fauziyah, F., Wang, Z. & Joy, G. (2022). Knowledge Management Strategy for Handling Cyber Attacks in E-Commerce with Computer Security Incident Response Team (CSIRT). Journal of Information Security, [online] 13(4), pp.294–311. doi:https://doi.org/10.4236/jis.2022.134016.

[33]. Gheyas, I.A. & Abdallah, A.E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. Big Data Analytics, 1(1). doi:https://doi.org/10.1186/s41044-016-0006-0.

[34]. Golightly, L., Modesti, P., Garcia, R. & Chang, V. (2023). Securing Distributed Systems: A Survey on Access Control Techniques for Cloud, Blockchain, IoT and SDN. Cyber Security and Applications, p.100015. doi:https://doi.org/10.1016/j.csa.2023.100015.

[35]. Grobler, M., Gaire, R. & Nepal, S. (2021). User, Usage and Usability: Redefining Human Centric Cyber Security. Frontiers in Big Data, 4. doi:https://doi.org/10.3389/fdata.2021.583723.

[36]. Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computernetworks, 169, 107094. (https://doi.org/10.1016/j.comnet.2019.107094).

[37]. Hammouchi, H., Cherqi, O., Mezzour, G., Ghogho, M., & El Koutbi, M. (2019). Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time. Procedia Computer Science, 151, 1004-1009. https://doi.org/10.1016/j.procs.2019.04.141

[38]. Hani Alshahrani, Khan, A., Rizwan, M., Saleh, M., Sulaiman, A. & Luige Vladareanu (2023). Intrusion Detection Framework for Industrial Internet of Things Using Software Defined Network. 15(11), pp.9001–9001. doi:https://doi.org/10.3390/su15119001.

[39]. Hotz, V.J., Bollinger, C.R., Komarova, T., Manski, C.F., Moffitt, R.A., Nekipelov, D., Sojourner, A. & Spencer, B.D. (2022). Balancing data privacy and usability in the federal statistical system. Proceedings of the National Academy of Sciences, 119(31). doi:https://doi.org/10.1073/pnas.2104906119.

[40]. Hu, S., Hsu, C. & Zhou, Z. (2021). Security Education, Training, and Awareness Programs: Literature Review. Journal of Computer Information Systems, pp.1–13. doi:https://doi.org/10.1080/08874417.2021.1913671.

[41]. Hunker, J. & Probst, C. (2021). Insiders and Insider Threats An Overview of Definitions and Mitigation Techniques. [online] Available at: https://isyou.info/jowua/papers/jowua-v2n1-1.pdf.

[42]. Hussain, S., Ahmad, M.B. & Uddin Ghouri, S.S. (2020). Advance Persistent Threat—A Systematic Review of Literature and Meta-Analysis of Threat Vectors. Advances in Computer, Communication and Computational Sciences, pp.161–178. doi:https://doi.org/10.1007/978-981-15-4409-5_15.

[43]. Ibrahim, A., Thiruvady, D., Schneider, J. G., &Abdelrazek, M. (2020). The challenges of leveraging threat intelligence to stop data breaches. Frontiers in Computer Science, 2, 36. (https://doi.org/10.3389/fcomp.2020.00036).

[44]. Illiashenko, O., Kharchenko, V., Babeshko, I., Fesenko, H. & Di Giandomenico, F. (2023). Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection. Entropy, [online] 25(8), p.1123. doi:https://doi.org/10.3390/e25081123.

[45]. Imperva (2022). Cybersecurity Risk Management | Frameworks, Analysis & Assessment | Imperva. [online] Learning Center. Available at: https://www.imperva.com/learn/data-security/cybersecurity-risk-management/.

[46]. Indu, I., Anand, P.M.R. & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering Science and Technology, an International Journal, [online] 21(4), pp.574–588. doi:https://doi.org/10.1016/j.jestch.2018.05.010.

[47]. Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. InformationSystemsFrontiers,1-22. (https://link.springer.com/article/10.1007/s10796-020-10044-1)

[48]. Jakóbik, A., (2016). Big data security. Resource Management for Big Data Platforms: Algorithms, Modelling, and High-Performance Computing Techniques, pp.241-261.

[49]. Jorge, C., Pereira Da Silva, A. and Lopes Cardoso, H. (2020). FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO Detecting and Protecting Personally Identifiable Information through Machine Learning Techniques. [online] Available at: https://repositorio-aberto.up.pt/bitstream/10216/129033/2/415776.pdf.

[50]. Jorge, C., Pereira Da Silva, A. & Lopes Cardoso, H. (2020). FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO Detecting and Protecting Personally Identifiable Information through Machine Learning Techniques. [online] Available at: https://repositorio-aberto.up.pt/bitstream/10216/129033/2/415776.pdf.

[51]. Kaloudi, N. & Li, J. (2020). The AI-Based Cyber Threat Landscape. ACM Computing Surveys (CSUR), 53(1), pp.1–34. doi:https://doi.org/10.1145/3372823.

[52]. Katarahweire, M., Bainomugisha, E. & Mughal, K.A. (2020). Data Classification for Secure Mobile Health Data Collection Systems. Development Engineering, 5, p.100054. doi:https://doi.org/10.1016/j.deveng.2020.100054.

[53]. Khraisat, A., Gondal, I., Vamplew, P. &Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, [online] 2(1), pp.1–22. doi:https://doi.org/10.1186/s42400-019-0038-7.

[54]. Kilincer, I. F., Ertam, F., &Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. Computer Networks, 188, 107840. https://doi.org/10.1016/j.comnet.2021.107840

[55]. Kotsias, J., Ahmad, A. & Scheepers, R. (2022). Adopting and Integrating Cyber-Threat Intelligence in a Commercial Organisation. European Journal of Information Systems, [online] pp.1–17. doi:https://doi.org/10.1080/0960085x.2022.2088414.

[56]. Kuppusamy, P., Samy, G.N., Maarop, N., Magalingam, P., Kamaruddin, N., Shanmugam, B. & Perumal, S. (2020). Systematic Literature Review of Information Security Compliance Behaviour Theories. Journal of Physics: Conference Series, 1551, p.012005. doi:https://doi.org/10.1088/1742-6596/1551/1/012005.

[57]. Kuppusamy, P., Samy, G.N., Maarop, N., Magalingam, P., Kamaruddin, N., Shanmugam, B. & Perumal, S. (2020). Systematic Literature Review of Information Security Compliance Behaviour Theories. Journal of Physics: Conference Series, 1551, p.012005. doi:https://doi.org/10.1088/1742-6596/1551/1/012005.

[58]. Lapin, K. &Šiurkus, M. (2022). Balancing Usability and Security of Graphical Passwords. Digital Interaction and Machine Intelligence, pp.153–160. doi:https://doi.org/10.1007/978-3-031-11432-8_15.

[59]. Lennartsson, M., Kävrestad, J. &Nohlberg, M. (2021). Exploring the meaning of usable security – a literature review. Information & Computer Security, ahead-of-print(ahead-of-print). doi:https://doi.org/10.1108/ics-10-2020-0167.

[60]. Li, S.-C., Chen, Y.-W. & Huang, Y. (2021). Examining Compliance with Personal Data Protection Regulations in Interorganizational Data Analysis. Sustainability, 13(20), p.11459. doi:https://doi.org/10.3390/su132011459.

[61]. Liu, C., Peng, Z. & Wu, L. (2016). Role of Time-Domain Based Access Control Model. Journal of Software Engineering and Applications, 09(02), pp.57–62. doi:https://doi.org/10.4236/jsea.2016.92004.

[62]. Maha, M. &Althobaiti (2016). ASSESSING USABLE SECURITY OF MULTIFACTOR AUTHENTICATION. [online] Available at: https://core.ac.uk/download/pdf/77028828.pdf.

[63]. Manikandakumar, M. & Ramanujam, E., (2018). Security and Privacy Challenges in Big Data Environment. In Handbook of Research on Network Forensics and Analysis Techniques (pp. 315-325). IGI Global.

[64]. Marcos de Lima, A.O. dos Santos &Pujolle, G. (2009). A survey of survivability in mobile ad hoc networks. IEEE Communications Surveys and Tutorials, 11(1), pp.66–77. doi:https://doi.org/10.1109/surv.2009.090106.

[65]. Marotta, A. & Madnick, S.E. (2020). Analyzing the Interplay Between Regulatory Compliance and Cybersecurity (Revised). SSRN Electronic Journal. doi:https://doi.org/10.2139/ssrn.3569902.

[66]. Mijwil, M.M., Doshi, R., Hiran, K.K., Unogwu, O.J. & Bala, I. (2023). MobileNetV1-Based Deep Learning Model for Accurate Brain Tumor Classification. Mesopotamian Journal of Computer Science, [online] 2023, pp.32–41. doi:https://doi.org/10.58496/MJCSC/2023/005.

[67]. Moghadam, R.S. & Colomo-Palacios, R., (2018). Information security governance in big data environments: A systematic mapping. Procedia computer science, 138, pp.401-408.

[68]. Mohamed, A.K.Y.S., Auer, D., Hofer, D. and Küng, J. (2022). A systematic literature review for authorization and access control: definitions, strategies and models. International Journal of Web Information Systems, 18(2). doi:https://doi.org/10.1108/ijwis-04-2022-0077.

[69]. Mohammed, A.A. (2015). Design and Implementation of Network Intrusion Detection System Based on Embedded System. www.academia.edu. [online] Available at: https://www.academia.edu/74376631/Design_and_Implementation_of_Network_Intrusion_Detection_System_Based_on_Embedded_System [Accessed 21 Dec. 2023].

[70]. Mohsin, J.K., Han, L., Hammoudeh, M. & Hegarty, R. (2017). Two Factor Vs Multi-factor, an Authentication Battle in Mobile Cloud Computing Environments. Proceedings of the International Conference on Future Networks and Distributed Systems. doi:https://doi.org/10.1145/3102304.3102343.

[71]. Moreno, J., Serrano, M.A. & Fernández-Medina, E., (2016). Main issues in big data security. Future Internet, 8(3), p.44.

[72]. Omar, M. (2021). Insider threats: Detecting and controlling malicious insiders. [online] Available at: https://scholar.archive.org/work/ezd3ndyijnbh3hzgdqpcuarf7u/access/wayback/http://www.saintleo.edu /media/972028/insider_threats.pdf [Accessed 21 Dec. 2023].

[73]. Opoku, A., Ahmed, V. &Akotia, J., (2016). Choosing an appropriate research methodology and method. Research methodology in the built environment: A selection of case studies, 1, pp.30-43.

[74]. Ørngreen, R. & Levinsen, K.T., (2017). Workshops as a research methodology. Electronic Journal of E-learning, 15(1), pp.70-81.

[75]. Otoom, A.A. (2014). A holistic cyber security implementation framework. www.academia.edu. [online] Available at: https://www.academia.edu/57832038/A_holistic_cyber_security_implementation_framework [Accessed 21 Dec. 2023].

[76]. Paja, E., Dalpiaz, F. and Giorgini, P. (2015). Modelling and reasoning about security requirements in socio-technical systems. Data & Knowledge Engineering, 98, pp.123–143. doi:https://doi.org/10.1016/j.datak.2015.07.007.

[77]. Palanisamy, V., &Thirunavukarasu, R. (2019). Implications of big data analytics in developing healthcare frameworks–A review. Journal of King Saud University-Computer and InformationSciences, 31(4), 415-425(https://doi.org/10.1016/j.jksuci.2017.12.007).

[78]. Phan, K. (2018). Implementing Resiliency of Adaptive Multi-Factor Authentication Systems. [online] p.65. Available at: https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1095&context=msia_etds.

[79]. Ponemon, I. (2012). 2012 Cost of Cyber Crime Study: United States Sponsored by HP Enterprise Security. [online] Available at: https://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.

[80]. Rajasekar, D. & Verma, R., (2013). Research methodology. Archers & Elevators Publishing House.

[81]. Reiley, D.H. and Rao, J.M. (2012). The Economics of Spam: Externalities, Market Institutions, and Strategic Games. SSRN Electronic Journal. doi:https://doi.org/10.2139/ssrn.2061865.

[82]. Riaz, S., Khan, A.H., Haroon, M., Latif, S. & Bhatti, S., (2020), August. Big data security and privacy: Current challenges and future research perspective in cloud environment. In 2020 International Conference on Information Management and Technology (ICIMTech) (pp. 977-982). IEEE.

[83]. Rosati, P., Gogolin, F. & Lynn, T. (2020). Cyber-Security Incidents and Audit Quality. European Accounting Review, pp.1–28. doi:https://doi.org/10.1080/09638180.2020.1856162.

[84]. Roy, A., Banerjee, A., & Bhardwaj, N. (2021). A Study on Google Cloud Platform (GCP) and Its Security. Machine Learning Techniques and Analytics for Cloud Security, 313-338.(https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119764113.ch15).

[85]. Sabillon, R., Serra-Ruiz, J., Cavaller, V. & Cano, J. (2017). A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). 2017 International Conference on Information Systems and Computer Science (INCISCOS). [online] doi:https://doi.org/10.1109/inciscos.2017.20.

[86]. Sachdev, A. & Bhansali, M. (2013). Enhancing Cloud Computing Security using AES Algorithm. International Journal of Computer Applications, [online] 67(9), p.19. Available at: https://www.academia.edu/70519709/Enhancing_Cloud_Computing_Security_using_AES_Algorithm [Accessed 19 Dec. 2023].

[87]. Sachdev, A. & Bhansali, M. (2013). Enhancing Cloud Computing Security using AES Algorithm. International Journal of Computer Applications, [online] 67(9), p.19. Available at: https://www.academia.edu/70519709/Enhancing_Cloud_Computing_Security_using_AES_Algorithm [Accessed 19 Dec. 2023].

[88]. Saeed, S., Suayyid, S.A., Al-Ghamdi, M.S., Al-Muhaisen, H. &Almuhaideb, A.M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors, [online] 23(16), p.7273. doi:https://doi.org/10.3390/s23167273.

[89]. Saleem, H., & Naveed, M. (2020). SoK: Anatomy of data breaches. Proc. Priv. Enhancing Technol., 2020(4), 153-174. DOI 10.2478/popets-2020-0067

[90]. Salleh, K.A. & Janczewski, L., (2016). Technological, organizational and environmental security and privacy issues of big data: A literature review. Procedia computer science, 100, pp.19-28.

[91]. Say, G., & Vasudeva, G. (2020). Learning from digital failures? The effectiveness of firms' divestiture and management turnover responses to data breaches. Strategy Science, 5(2), 117-142. (https://doi.org/10.1287/stsc.2020.0106).

[92]. Scarfone, K. & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). [online] csrc.nist.gov. Available at: https://csrc.nist.gov/pubs/sp/800/94/final.

[93]. Scheurich, J., (2014). Research method in the postmodern. Routledge.

[94]. Shah, G., Shirke, S., Sawant, S. and Dandawate, Y.H. (2015). Palm vein pattern-based biometric recognition system. International Journal of Computer Applications in Technology, 51(2), p.105. doi:https://doi.org/10.1504/ijcat.2015.068921.

[95]. Shaikh, R. & Sasikumar, M. (2015). Data Classification for Achieving Security in Cloud Computing. Procedia Computer Science, 45, pp.493–498. doi:https://doi.org/10.1016/j.procs.2015.03.087.

[96]. Shanai Ardi, Sandahl, K. & Magnus Hellström (2023). A Case Study of Introducing Security Risk Assessment in Requirements Engineering in a Large Organization. SN computer science, 4(5). doi:https://doi.org/10.1007/s42979-023-01968-x.

[97]. Sharma, R.C. (2022). Cybersecurity Management for Incident Response. Romanian Cyber Security Journal. [online] Available at: https://www.academia.edu/79091089/Cybersecurity_Management_for_Incident_Response [Accessed 21 Dec. 2023].

[98]. Shihab, L.A., 2020. Technological tools for data security in the treatment of data reliability in big data environments. International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, 11(9), pp.1-13.

[99]. Shirish, T.S., (2014). Research methodology in education. Lulu. com.

[100]. Singh, A. and Sharma, A. (2021). A systematic literature review on insider threats. [online] Available at: https://arxiv.org/pdf/2212.05347 [Accessed 19 Dec. 2023].

[101]. Snyder, H., (2019). Literature review as a research methodology: An overview and guidelines. Journal of business research, 104, pp.333-339.

[102]. Stallings, W., Columbus, B., New, I., San, Y., Hoboken, F., Cape, A., Dubai, T., Madrid, L., Munich, M., Montréal, P., Delhi, T., São, M., Sydney, P., Kong, H., Singapore, S. and Tokyo, T. (2020). CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE SEVENTH EDITION GLOBAL EDITION. [online] Available at: https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf.

[103]. Stallings, W., Columbus, B., New, I., San, Y., Hoboken, F., Cape, A., Dubai, T., Madrid, L., Munich, M., Montréal, P., Delhi, T., São, M., Sydney, P., Kong, H., Singapore, S. & Tokyo, T. (2020). CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE SEVENTH EDITION GLOBAL EDITION. [online] Available at: https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf.

[104]. Sun, Y., Zhang, J., Xiong, Y. & Zhu, G. (2019). Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks, [online] 10(7), p.190903. doi:https://doi.org/10.1155/2014/190903.

[105]. Sutton, M. (2020). The Cyber Threat Landscape. The ITP Journal. [online] Available at: https://www.academia.edu/42810651/The_Cyber_Threat_Landscape [Accessed 19 Dec. 2023].

[106]. Synopsys Elizabeth (2019). What is Security Risk Assessment and How Does It Work? | Synopsys. [online] Synopsys.com. Available at: https://www.synopsys.com/glossary/what-is-security-risk-assessment.html.

[107]. Tang, Z. & Pan, Y., (2015). Big Data Security Management. In Handbook of Research on Trends and Future Directions in Big Data and Web Intelligence (pp. 53-66). IGI Global.

[108]. Tankard, C. (2015). Data classification – the foundation of information security. Network Security, 2015(5), pp.8–11. doi:https://doi.org/10.1016/s1353-4858(15)30038-6.

[109]. Tate, J., Beck, P., Clemens, P., Freitas, S., Gatz, J., Girola, M., & Walker, J. (2013). IBM and Cisco: together for a world class data center. IBM Redbooks.(https://books.google.com.pk/books?hl=en&lr=&id=DHjJAgAAQBAJ&oi=fnd&pg=PP1&dq=Real-World+Example:+Cisco&ots=-e0xCk6m4n&sig=YEHAKlEDUzUX3VUKB24LEerNYhw&redir_esc=y#v=onepage&q=Real-World%20Example%3A%20Cisco&f=false).

[110]. Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., &Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102. (https://doi.org/10.3390/app10124102).

[111]. Thapa, S. & Dissanayaka, A. (2020). THE ROLE OF INTRUSION DETECTION/PREVENTION SYSTEMS IN MODERN COMPUTER NETWORKS: A REVIEW. [online] Available at: https://www.micsymposium.org/mics_2020_Proceedings/MICS2020_paper_1.pdf.

[112]. Thomas, J. E. A Case Study Analysis of the Equifax Data Breach. (https://www.researchgate.net/profile/Jason-Thomas-21/publication/337916068_A_Case_Study_Analysis_of_the_Equifax_Data_Breach_1_A_Case_Study_Analysis_of_the_Equifax_Data_Breach/links/5df2f9804585159aa4793667/A-Case-Study-Analysis-of-the-Equifax-Data-Breach-1-A-Case-Study-Analysis-of-the-Equifax-Data-Breach.pdf.)

[113]. Ullah, Z., Al-Turjman, F., Mostarda, L., & Gagliardi, R. (2020). Applications of artificial intelligence and machine learning in smart cities. Computer Communications, 154, 313-323. (https://doi.org/10.1016/j.comcom.2020.02.069).

[114]. Williamson, J. & Curran, K. (2021). Best Practice in Multi-factor Authentication. Semiconductor Science and Information Devices, 3(1). doi:https://doi.org/10.30564/ssid.v3i1.3152.

[115]. Wittig, A., & Wittig, M. (2023). Amazon Web Services in Action: An In-depth Guide to AWS. Simon and Schuster.(https://books.google.com.pk/books?hl=en&lr=&id=joK3EAAAQBAJ&oi=fnd&pg=PA1&dq=Case+Study:+Amazon+Web+Services+(AWS)&ots=DsMlRycCo-&sig=IRXUaYGeiLRtnScbGau0nGvdPjQ&redir_esc=y#v=onepage&q=Case%20Study%3A%20Amazon%20Web%20Services%20(AWS)&f=false).

[116]. Xu, D. & Zheng, W. (2022). Application of Data Encryption Technology in Network Information Security Sharing. Security and Communication Networks, 2022, pp.1–6. doi:https://doi.org/10.1155/2022/2745334.

[117]. Yazdinejad, A., Dehghantanha, A., Parizi, R.M., Srivastava, G. &Karimipour, H. (2023). Secure Intelligent Fuzzy Blockchain Framework: Effective Threat Detection in IoT Networks. Computers in Industry, 144, p.103801. doi:https://doi.org/10.1016/j.compind.2022.103801.

[118]. Yazdinejad, A., Kazemi, M., Parizi, R.M., Dehghantanha, A. &Karimipour, H. (2022). An ensemble deep learning model for cyber threat hunting in industrial internet of things. Digital Communications and Networks. doi:https://doi.org/10.1016/j.dcan.2022.09.008.

[119]. Yu, Y. (2022). Encryption Technology for Computer Network Data Security Protection. Security and Communication Networks, [online] 2022, p.e1789222. doi:https://doi.org/10.1155/2022/1789222.

[120]. Yuan, T., (2017). Towards the development of best data security for big data.

[121]. ZAMFIROIU, A. & SHARMA, R.C. (2022). Cybersecurity Management for Incident Response. Romanian Cyber Security Journal, 4(1), pp.69–75. doi:https://doi.org/10.54851/v4i1y202208.

[122]. Zhou, X. & Tang, X. (2011). Research and implementation of RSA algorithm for encryption and decryption. Proceedings of 2011 6th International Forum on Strategic Technology. [online] Available at: https://www.semanticscholar.org/paper/Research-and-implementation-of-RSA-algorithm-for-Zhou-Tang/a5d426d6f4bd5dc3311f0c994f642cf1f5de0488.