SCHOOL OF COMPUTING, UUM COLLEGE OF ARTS AND SCIENCES

SKIC2113 CRYPTOGRAPHY

(SEMESTER A222)

GROUP ASSIGNMENT 1:

CASE STUDY REPORT

TOPIC:

HACKERS WHO STOLE 10TB WESTERN DIGITAL DATA DEMAND' 8 FIGURE' RANSOM

LECTURER:

PROF. MADYA TS. DR. NORLIZA BINTI KATUK

PREPARED BY:

GROUP BLOWFISH

NAME	MATRIC NO.
AINUR HANIM BINTI ABDUL HALIM	288091
TAN ZHI XIAN	284333
NURIN ANDRIANA BINTI MOHD SUBRI	287957
NURIN IZZAH BINTI ISHAK	288063

DATE OF SUBMISSION:

5 JUNE 2023

TABLE OF CONTENTS

SECTION 1: INTRODUCTION

1.1 Overview

Western Digital is an American technology company based in San Jose, California, specializing in data storage solutions. With a mission to meet the diverse data storage needs of individuals, businesses, and enterprises, Western Digital excels in two key areas of business. They offer an extensive range of data storage solutions, encompassing hard disk drives (HDDs), solid-state drives (SSDs), network-attached storage (NAS) systems, and memory cards. Additionally, their expertise extends to providing optimized data center solutions for enterprises and cloud service providers, empowering them to efficiently manage data-intensive applications.

Complementing its exceptional product offerings, Western Digital provides an array of services, such as data recovery services to retrieve data from damaged or failed storage devices, technical support for seamless product integration, warranty, and RMA services for hassle-free replacements or repairs, and data security and encryption services to safeguard sensitive information. With a comprehensive portfolio of cutting-edge solutions and services, Western Digital remains at the forefront of the data storage industry, meeting the evolving needs of customers worldwide.

According to the case that has been extensively researched, the primary focus revolves around a group of hackers who managed to steal a staggering 10TB of data from Western Digital. Their audacious move is accompanied by an equally audacious demand, which is an eight-figure ransom. What makes this situation even more concerning is that the stolen data includes a significant amount of customer information. The hackers' main objective seems to be to earn financial gains by letting the company nervous to prevent public exposure of the data they have obtained.

According to the news report from The Economic Times, Western Digital fell victim to a ransomware cyberattack on 26 March 2023 *(Ciso, 2023)*. During this attack, unauthorized individuals gained access to a copy of a database containing the personal details of customers associated with an online business. As a result of this breach, Western Digital took the precautionary measure of temporarily suspending account access for affected customers and promptly notified them about the incident.

The hackers, driven by their desire to keep their stolen data hidden, have resorted to demanding a substantial ransom. To prove their capabilities and infiltrate corporate systems, they have presented evidence in the form of a file digitally signed with Western Digital's code-signing certificate. Additionally, it has come to light that the hackers have obtained the phone numbers of several business leaders, leading to automated voicemails with the executives' names being left. Screenshots provided by the hackers reveal their access to data from a PrivateArk instance, internal emails, files from a Box account, and even a snapshot of a conference call involving Western Digital's top information security officer *(Krasnogolovy, 2023)*.

Given that the corporate email system is temporarily inaccessible, the hackers have attempted to establish contact with Western Digital using personal email addresses, with their primary motivation appearing to be financial gain. If their demands are not met, they have made it clear that they will take action and demand a one-time payment. Despite denying any intentional targeting of Western Digital and withholding personal or organizational information, the hackers' ultimate threat involves posting the stolen data on their own website unless Western Digital responds accordingly.

Surprisingly, Western Digital has not responded to the hackers' assertions nor provided any additional information about the nature of the data breach, including the potential inclusion of customer information. Equally concerning is the hackers' refusal to disclose specifics regarding the types of client data they have stolen or the methods they employed to penetrate the network. Although the hackers claim no direct association with the ALPHV or BlackCat ransomware gang, their intentions to publicly release the stolen data loom large if Western Digital fails to comply with their demands.

1.2 Security Properties Violated

Data confidentiality is the first security property that has been broken in this instance. Examples of allegations connected to this security measure include the assertion that hackers were able to breach Western Digital's system and steal a massive 10TB of data, including sensitive information such as client data and trade secrets *(Franceschi-Bicchierai, 2023)*. This unauthorized access and tampering with sensitive data demonstrate a breach of data confidentiality. Interestingly, the hacker claimed that their goal in breaking into

Western Digital was to make money, so they chose not to use malware to lock the company's files.

The next security property that can relate to this case is data integrity. The hackers sent files to TechCrunch that appeared to be digitally signed with a Western Digital code-signing certificate. However, upon closer examination, researchers discovered that the hackers had compromised the data integrity by altering and fabricating files to make them appear authentic. The phony signature, although closely resembling Western Digital's original signature, was ultimately proven to be fake *(Saw, 2023)*.

The violation of availability is also a concern. The hackers may have gained control over the data or encrypted it, thereby preventing Western Digital from accessing or using it until the situation is resolved. This obstruction in availability poses serious consequences for the company's operations, potentially disrupting their normal workflow and impeding their ability to provide services to their customers. The unavailability of critical data and systems can have far-reaching implications, leading to delays, operational inefficiencies, and even financial losses.

Furthermore, there is a breach of access control in this case. The unauthorized individuals were able to gain access to consumer data due to the compromise of the Western Digital database copy, indicating a breakdown in access control systems *(CS Staff, 2023)*. This security flaw highlights the absence of appropriate access restrictions, which allowed unauthorized individuals to view sensitive data.

Extortion also comes into play as a violated security property in this scenario *(The Hacker News, 2023)*. The hackers, who are associated with the ransomware group ALPHV, which is also known as BlackCat, demanded a substantial ransom payment of "minimum 8 figures" to prevent the disclosure of the stolen data. This extortion attempt involved threats of revealing the hacked data in exchange for a significant sum of money, potentially causing financial and reputational harm to the company.

1.3 Consequences of The Attacks

The consequences of the attacks on Western Digital are far-reaching and encompass various negative impacts.

One significant consequence is the potential for substantial financial loss. The theft of the data could cause the company to lose a lot of money. As seen in the case of the temporary shutdown of services like My Cloud, the need for system repairs and security measures has caused interruptions in regular company operations. This disruption inconveniences customers and may result in financial losses for the company. The implementation of enhanced security measures and the restoration of services can also entail additional operating expenditures. Other than that, in order to stop future attacks, they might have to pay for investigations, legal fees, and security measures. Besides, the hackers have demanded an "8-figure" ransom from Western Digital. The business might have to pay a sizable quantity of money to get their data back if the hackers demand a ransom in exchange for returning the stolen information. Firstly, there is no guarantee that paying the ransom will result in the safe return of the stolen data or prevent further misuse or distribution of the data. Additionally, paying the ransom can encourage future attacks and incentivize hackers to target the company again or other organizations. It can also create a reputation for the company as an easy target for ransom demands, attracting further malicious actors. Finally, paying a significant ransom can have a significant financial impact on the company's resources, affecting its financial stability and long-term viability. Moreover, this could inspire more assaults and be interpreted as encouraging bad behavior.

One of the most concerning consequences is data exposure and privacy breach, primarily focusing on the compromise of customer data. The hackers obtained sensitive information such as partial credit card numbers, names, email addresses, billing and delivery addresses, and hashed passwords. This breach of customer data has severe implications for privacy, increasing the risk of identity theft, phishing scams, and other malicious activities. The stolen data can be exploited by hackers for privacy violations, identity theft, and other criminal acts, further impacting the affected individuals Therefore, the attacks have also resulted in the loss of reputation and trust for Western Digital. Both existing and potential customers may now harbor concerns about the security of their data and hesitate to engage with the company's services. The breach of confidentiality and potential for repeat incidents create fear among customers, eroding their trust in Western Digital as a reliable provider of digital storage solutions. This loss of trust can lead to decreased customer loyalty and ultimately impact the company's bottom line *(Saw, 2023)*.

SECTION 2: ANALYSIS OF THE ATTACK

2.1 Incident Investigation

In the Western Digital ransomware data breach incident, the attackers employed a unique "ransomware attack with data theft and extortion." Unlike traditional ransomware attacks that encrypt files and demand payment for their decryption, APLHV took a different approach. Instead, they managed to infiltrate Western Digital's systems and stole approximately ten terabytes of data *(CS Staff, 2023).*

The stolen data encompassed a variety of sensitive information belonging to Western Digital's online store customers. This includes personally identifiable data (PII) such as names, addresses, phone numbers, email addresses, hashed passwords, and partial credit card numbers. This type of PII is precious to cyber criminals as it can be used for fraud, identity theft, or to make money by being sold on the dark web.

Figure 1: First Statement of hackers about the attack on Western Digital

In addition to the customer data, the attackers claimed access to critical assets within Western Digital's infrastructure. This included the company's code-signing keys, which verify the authenticity and integrity of software and updates released by Western Digital. Having control over these keys could enable attackers to distribute malicious software or updates that appear to be legitimate, bypassing security measures.

Furthermore, the attackers stated that they had obtained unlisted corporate phone numbers, providing them with avenues for unauthorized access or social engineering attacks. Additionally, they asserted having complete backup data from Western Digital's SAP Backoffice implementation, indicating they had access to sensitive internal systems and databases.

The attackers leaked some screenshots of the stolen data and the company's internal communications to exert pressure on Western Digital and increase the payment likelihood. By exposing snippets of the stolen information and internal discussions, they aimed to demonstrate their capability and willingness to disclose more sensitive data if their demands were unmet *(Waldman, 2023)*.

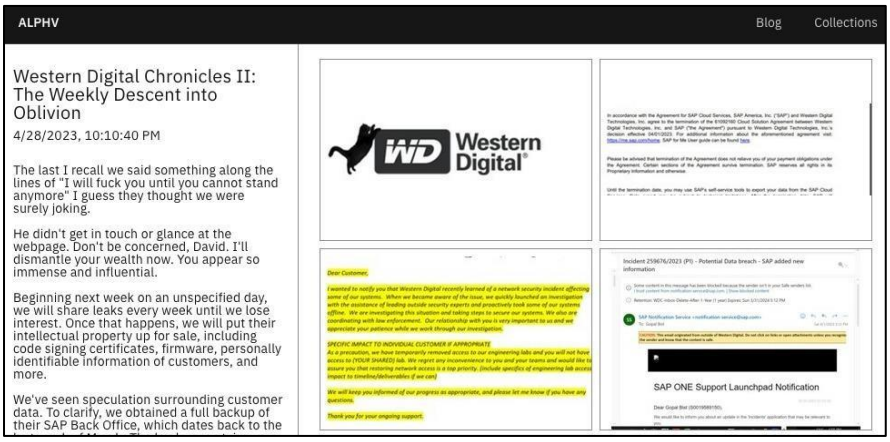

Figure 2: Second Statement published by ALPHV / Black Cat that threatens Western Digital to pay the ransom or face weekly data releases.

Overall, this incident showcased the evolving tactics used by cybercriminals, demonstrating that data theft and extortion can be just as damaging and threatening as traditional ransomware attacks. The stolen data and the potential compromise of critical assets like code-signing keys, unlisted phone numbers, and backup data posed significant risks to Western Digital's operations, customer trust, and overall security posture.

2.2 Attack Methodology

In the realm of cybersecurity, the battle between attackers and defenders' rages on, with attack methodologies becoming increasingly sophisticated and diverse. From ransomware attack ploys to technical exploits, understanding the intricacies of attack methodologies is vital for Western Digital organizations striving to safeguard their data and infrastructure. This section delves into the multifaceted world of attack methodologies, exploring the tactics, techniques, and strategies employed by malicious actors to breach security defenses and compromise sensitive information.

2.2.1 Launching Ways

In recent years, ransomware attacks have evolved to become more sophisticated and targeted, posing significant challenges for organizations worldwide. Below are the launching ways employed by ransomware attackers, focusing specifically on the case of Western Digital. By understanding the tactics used and the implications they have for the targeted organization, the company can gain insights into the evolving threat landscape and the urgent need for enhanced cybersecurity measures.

Firstly, modern ransomware attacks often involve targeted approaches known as "big-game hunting" or "human-operated attacks." These attackers extensively profile potential victims using databases and tools to identify specific targets based on location, industry, size, and revenue. Anonymous communication platforms facilitate secure collaboration among cybercriminal groups *(Franceschi-Bicchierai, 2023)*. Once a victim which Western Digital is identified and network access is gained, the attackers spend significant time infiltrating distinct parts of the network to locate sensitive data and compromise critical backups, making a recovery more complex. This deep access enables the ransomware actors to understand Western Digital's financial health and tailor ransom demands accordingly.

Moreover, in the case of Western Digital's infrastructure breach, hackers took advantage of vulnerabilities through a technique known as "web crawling." Web crawling is a process where automated software, known as web crawlers or bots, systematically browse WD webpages to gather information about their content. This information is then indexed, updated, and made accessible when users perform search queries. By utilizing this technique, ALPHV likely employed automated software or scripts to systematically

navigate through Western Digital's web pages, probing for security weaknesses. Once ALPHV identified these vulnerabilities, the hackers follow hyperlinks to discover new pages and expand their coverage by gaining unauthorized access to Western Digital's Microsoft Azure tenants, which are cloud-based resources provided by Microsoft. This unauthorized access allowed the hackers to assume the role of global administrators, granting them extensive control over Western Digital's Azure-based resources.

After that, the ransomware actors employ a tactic called "double extortion." In addition to encrypting the victim's data, they exfiltrate it from the network. This additional step provides cybercriminals with an alternative means of extortion, as they can threaten to publish or sell the stolen data on the dark web or exploit vulnerabilities in related systems. The implementation of double extortion has significantly amplified the pressure on victims to pay the ransom, leading to increased ransom demands and payouts.

In the case of the Western Digital data breach, the attackers went beyond encrypting data and employed additional tactics to demonstrate their capabilities and exert further pressure. They circulated a file bearing the digital signature of Western Digital's code-signing certificate, showcasing their ability to forge digital signatures and impersonate the company. This not only undermines trust in the company's software but also raises concerns about the integrity of future software updates. Additionally, the attackers disclosed phone numbers linked to multiple executives within the company, exposing sensitive information. The fact that some calls were redirected to automated voicemail systems, with voicemail greetings mentioning the executives' names, adds to the level of concern. It is crucial to note that these phone numbers were private, indicating a breach of internal security protocols *(Jefferson, 2020)*.

Western Digital serves as an example of how ransomware attackers' shifting strategies highlight the urgent need for businesses to improve their cybersecurity safeguards. The capacity to forge digital signatures, targeted approaches, and double extortion tactics present serious difficulties for victims and the business as a whole. The company must invest in proactive cybersecurity solutions as technology develops in order to defend its sensitive data, preserve customer confidence, and safeguard its reputation in a hostile digital environment.

2.2.2 Possible Ways to Do the Attack

In the current digital environment, organizations must contend with an expanding variety of cyber threats that have the potential to jeopardize critical data and disrupt operations. The threats that Western Digital specifically faces are examined in this essay, including phishing, distributed denial of service (DDoS), and social engineering attacks. The integrity of Western Digital's systems and the safety of its customers depend on understanding and addressing these risks.

Firstly, Western Digital customers have received phishing emails that appear to be from the company. The emails ask customers to change their passwords immediately and provide a link to a support page that looks like it belongs to Western Digital. The company has warned users to be on guard against phishing messages. Other than that, Western Digital might have an employee who accidentally clicks a malicious link or downloads an infected attachment in a phishing email. This may lead to the installation of malware on the computer of the recipient, the locking of the device by ransomware, or the release of personal information.

In the context of a Western Digital data breach, a DDoS attack could be a diversionary tactic. The attacker might launch a DDoS attack against the company's servers or network infrastructure to distract the security team and prevent them from detecting or responding to the data breach. By flooding the targeted WD system with a massive volume of incoming traffic, the attacker can exhaust the system's resources, such as bandwidth, processing power, or memory. This overload causes the system to become unresponsive or even crash, rendering it temporarily or utterly inaccessible to legitimate users.

Another significant risk faced by Western Digital is social engineering, whereby attackers exploit the vulnerabilities of employees to gain unauthorized access to systems or sensitive information. This tactic capitalizes on human error and the innate inclination to trust and assist others. Rather than targeting software vulnerabilities, social engineering leverages the unpredictability of legitimate user errors, making them more challenging to identify and prevent. Techniques such as phishing and manipulation can deceive employees into divulging confidential information or granting unauthorized access to critical systems. To combat this threat, Western Digital must invest in comprehensive employee training programs and cybersecurity awareness initiatives. By fostering a security-

conscious culture and implementing multi-layered security measures, including robust access controls and authentication protocols, the organization can mitigate the risks associated with human vulnerabilities *(Jefferson, 2020)*.

Western Digital faces an evolving cybersecurity landscape, where Phishing, DDoS, and social engineering assaults all pose serious dangers in the ever-evolving cybersecurity environment. Western Digital can preserve the information of its customers and fight against unauthorized access by aggressively resolving these issues. Western Digital will be able to preserve the confidence of its clients and strengthen its resistance to new cyber threats by putting in place consistent employee training programs, raising cybersecurity awareness, and installing effective monitoring and mitigation methods. Proactive actions are crucial to building a strong defense against hackers looking to exploit weaknesses and disrupt crucial activities in a world of technology that is continually growing.

2.3 Reasons Behind the Attack

The fusion of vulnerabilities and motives sets the stage for this cyber-attack, highlighting the critical importance of understanding their intertwined nature.

2.3.1 Vulnerabilities

Western Digital's data breach revealed serious flaws and system configuration errors in the organization's systems. Five aspects that may have led to the breach are examined in this analysis which are problems with Western Digital's My Cloud service, resource substitution vulnerabilities, poor key management, a lack of data backup and recovery procedures, and improper implementation of access controls. For Western Digital to bolster its cybersecurity defenses and reduce the danger of further intrusions, it is crucial to comprehend these aspects.

One significant factor is the network security incident that impacted Western Digital's My Cloud service. The extended downtime and potential exposure of vulnerabilities during this incident may have confused both the company and its customers, making them susceptible to further attacks. The use of the SMB protocol for local network access can be targeted by cybercriminals due to its exploitable code execution capabilities and access to sensitive data. Improved transparency and awareness of the extent of the

breach could have helped mitigate its impact *(Western Digital Provides Update on Network Security Incident | Western Digital, 2023)*.

Additionally, it was discovered that the SSD Dashboard software from Western Digital and SanDisk had a flaw that made it susceptible to possible man-in-the-middle attacks while downloading resources. Due to this weakness, there was a window of opportunity for attackers to intercept the transmission and download arbitrary files in place of the intended resources. Attackers could possibly insert and run malicious code by taking advantage of this vulnerability, posing serious threats to the security and integrity of systems. Western Digital and SanDisk can better protect their users from the potential risks associated with man-in-the-middle attacks and increase trust in their goods and services by prioritizing these security measures and routinely updating and patching their software *(WDC-19009 SanDisk and Western Digital SSD Dashboard Vulnerabilities | Western Digital, 2019)*.

Furthermore, the hackers' ability to digitally sign files using Western Digital's code-signing certificate exposes weaknesses in the company's key management practices and the risk of unauthorized access to digital signing capabilities. This breach undermines trust, allowing attackers to deceive users into running or installing malicious files. Effective key management, including secure storage and strong access controls, is crucial to prevent such exploits. Organizations must prioritize comprehensive key management strategies to protect cryptographic keys, mitigate unauthorized access, and maintain the integrity of digital signatures.

Next, the absence of dependable data backup and recovery mechanisms increased Western Digital's vulnerability to ransomware assaults. Because there were insufficient backups, the company was exposed to the possibility of data loss, which led them to think about paying ransoms to get hold of important records. The protracted outage during data restoration operations highlighted the necessity of thorough backup measures to reduce disruptions and monetary losses. Western Digital must have a proactive data backup and recovery plan to increase resilience, defend against ransomware attacks, and guarantee business continuity *(IANS, 2023)*. Western Digital can lessen the effects of breaches, decrease downtime, and uphold stakeholder trust by putting a priority on safe backups, offsite storage, and routine testing.

Lastly, through the improper setting of access controls inside the SAP back-office interface, the breach suggested unauthorized data access. Attackers may have been able to steal sensitive data and increase their privileges within the Western Digital application due to lax authentication and access control settings. The danger of unauthorized access and data compromise would have been reduced by putting tighter access control measures in place, such as correctly configured authentication systems and privileged account management.

In summary, the compromise of sensitive data by Western Digital was made possible by vulnerabilities and misconfigurations that were made public. Western Digital can reduce the risk of exploitation and protect the integrity of its systems by enhancing network security, resource verification mechanisms, key management procedures, data backup and recovery processes, and access controls. To keep a proactive and resilient cybersecurity posture, regular audits, ongoing personnel training, and continuous monitoring are also essential. Western Digital can rebuild confidence and ensure the privacy, integrity, and accessibility of its data and services by reflecting on the compromise and taking the necessary precautions.

2.3.2 Motivation

The primary motive of APLHV, as observed in their actions, is to generate financial gain through extortion. They employ ransomware attacks with data theft to achieve this objective. By stealing sensitive data from their victims, they acquire leverage to demand substantial ransom payments in exchange for returning or deleting the stolen information. This financial incentive serves as a driving force behind their attacks. In addition to their financial motivations, APLHV claims to have a political agenda. They specifically target Western Digital companies, accusing them of corruption and oppression. Their slogan, "We are not criminals; we are freedom fighters", suggests they perceive themselves as activists fighting against perceived injustices.

However, some security experts are skeptical of APLHV's ideological claims and view them as a cover for their underlying financial goals. These experts question the extent to which APLHV genuinely seeks to promote political change or expose corruption and oppression. Instead, they believe the group may exploit such claims to justify their criminal activities and garner support or sympathy from certain groups or individuals. It is worth

noting that discerning the true motivations and ideology of cybercriminal groups can be challenging, as they often operate covertly and anonymously. While APLHV may attempt to portray themselves as freedom fighters, the evidence of their actions is demanding ransoms, stealing data, and engaging in cybercriminal activities. Suggests that their primary focus is financial gain.

Ultimately, the exact motives and intentions of APLHV may remain a subject of speculation, as cybercriminal groups often employ a mix of ideological rhetoric and financial goals to achieve their objectives.

2.4 Perpetrator Identification

Figure 3: ALPHV / Black Cat ransomware group

According to BleepingComputer *(2023)*, the data breach at Western Digital is believed to have been orchestrated by the ransomware gang ALPHV, also known as BlackCat. ALPHV is a rising faction in the ransomware-as-a-service (RaaS) landscape that emerged in November 2021. Notably, the group has actively recruited former members of well-known ransomware groups such as REvil, BlackMatter, and DarkSide. ALPHV employed aggressive triple-extortion tactics in this case by leaking screenshots of internal emails, files, and video conferences related to Western Digital's response efforts following the cyberattack. They threatened to inflict severe damage on the company unless a ransom was paid. Despite the threats, Western Digital decided not to negotiate with ALPHV and has not commented on the attackers' claims.

SECTION 3: THE PROPOSED SOLUTION

3.1 Symmetric Key Encryption Protection

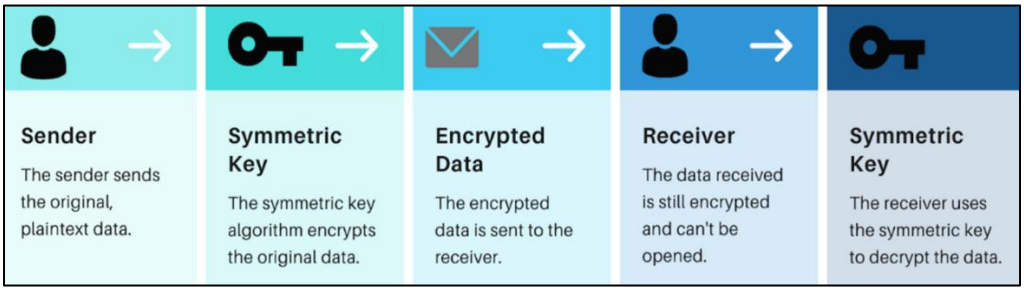

Figure 4: Symmetric key encryption process

Symmetric key cryptography, or private key cryptography, is a form of encryption Western Digital uses to protect data from unauthorized access. This encryption technique uses the same key for both encryption and decryption.

Symmetric key encryption offers a range of protections that safeguard data and ensure its confidentiality, secure transmission, file, and disk encryption, and privacy protection. Firstly, symmetric key encryption maintains confidentiality by transforming plaintext into ciphertext using a shared key. This encryption renders the data unintelligible to unauthorized individuals who may intercept it, as decryption requires the correct key.

Moreover, symmetric key encryption plays a crucial role in secure data transmission. Organizations like Western Digital can prevent eavesdropping and interception by malicious attackers, such as ransomware operators, by encrypting data before sending it over insecure networks or channels. Even if intercepted, the encrypted data remains unreadable without the decryption key.

Symmetric key encryption is a fundamental component of privacy protection. When transmitting sensitive data over a network, Western Digital can use symmetric key encryption to encrypt the data before transmission. This encryption prevents unauthorized individuals from intercepting or understanding the contents of the communication, thereby preserving the confidentiality of sensitive data. Privacy protection encompasses broader considerations concerning the protection of personal data and respect for individual privacy rights.

In conclusion, symmetric key encryption offers a variety of protections that are invaluable in the realm of data security. From ensuring confidentiality and secure data transmission to protecting files and disks, as well as privacy, symmetric key encryption serves as a robust defence mechanism, enabling organizations like Western Digital to safeguard their sensitive information from unauthorized access and maintain the confidentiality and integrity of their data.

3.2 Message Authentication Protection

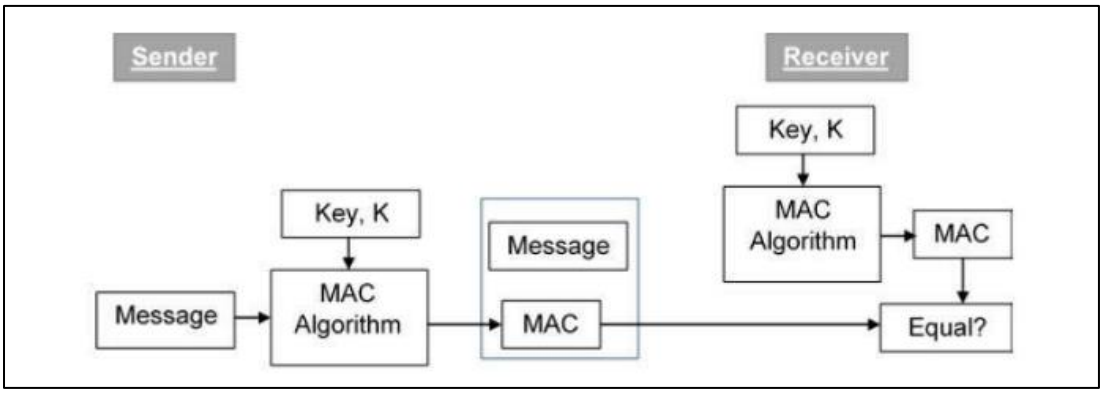

Figure 5: Message authentication process

Message authentication offers a range of protections that enhance data integrity, trust, and assurance within Western Digital's network and systems. These protections include integrity assurance, improving confidence and data assurance, non-repudiation, tamper detection, and protection against replay attacks.

One of the primary benefits of message authentication is ensuring data integrity. By employing cryptographic algorithms such as HMAC (Hash-based Message Authentication Code) or digital signatures, Western Digital can verify that data has not been altered or tampered with during transmission. This safeguard guarantees the integrity of critical information, ensuring that it remains unchanged and trustworthy.

In addition to integrity, message authentication is crucial in enhancing trust and data assurance. By assuring clients that their data is protected from tampering and unauthorized changes, Western Digital demonstrates a commitment to data integrity and security. This helps bolster user and consumer confidence in the company's services and products.

Furthermore, message authentication mechanisms provide non-repudiation, preventing senders from denying their responsibility for specific messages or data. Through digital signatures, Western Digital can maintain evidence that a letter was sent by a particular sender, thereby preventing false claims of non-involvement. This accountability and non-repudiation contribute to a more secure and reliable communication environment.

Tamper detection is another significant protection provided by message authentication. Western Digital can detect whether data has been altered during transmission or while being stored. Any discrepancies are identified by recalculating the Message Authentication Codes (MACs) for the saved data and comparing them with the stored values. This process ensures the integrity and validity of the data and aids in the identification of potential security breaches.

Message authentication also safeguards Western Digital against replay attacks. These attacks involve intercepting and resending legitimate data to gain unauthorized access or deceive the system. The company can detect and reject replayed data by incorporating timestamps or sequence numbers in authenticated messages, preventing potential security breaches.

In conclusion, message authentication provides a range of essential protections to Western Digital's network and systems. From ensuring data integrity and enhancing trust to providing non-repudiation, tamper detection, and protection against replay attacks, these mechanisms play a vital role in maintaining the security and reliability of data communications. By implementing robust message authentication protocols, Western Digital can safeguard its infrastructure and provide users with a secure and trustworthy environment for their data.

3.3 Analyzation and Demonstration of Cryptographic Techniques

In today's digital landscape, data security is of paramount importance for organizations. Encryption and message authentication are crucial techniques that Western Digital can employ to protect its sensitive data from unauthorized access and ensure data integrity. This part of the case study report provides an overview of two main techniques, namely symmetric key encryption, and message authentication, along with practical demonstrations of their implementation.

3.3.1 Symmetric Key Encryption

Western Digital can employ symmetric key encryption to encrypt its sensitive data, such as customer databases, financial records, and intellectual property. This encryption can be applied at rest (stored data) and in transit (data being transmitted over networks). The encryption keys must be securely generated, stored, and managed. Western Digital should use robust key management practices, including secure key storage, regular key rotation, and strict access controls. In the event of this ALPHV ransomware attack, even if the attackers gain access to the encrypted data, they will not be able to decrypt it without the encryption keys, rendering the stolen data useless to them. Full Disk Encryption (FDE) and Cloud Storage Encryption are the two primary methods Western Digital can utilize.

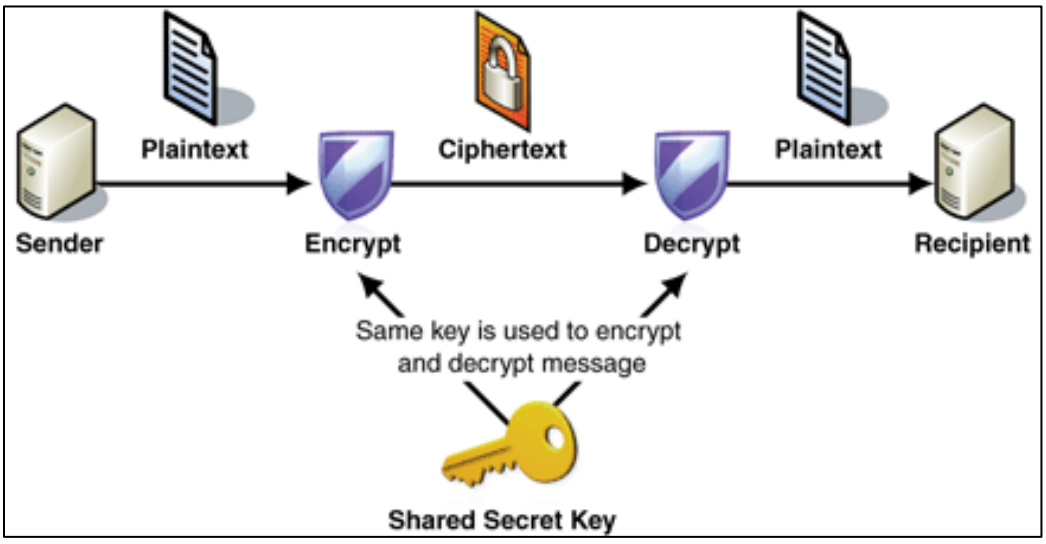

Figure 6: Symmetric key encryption

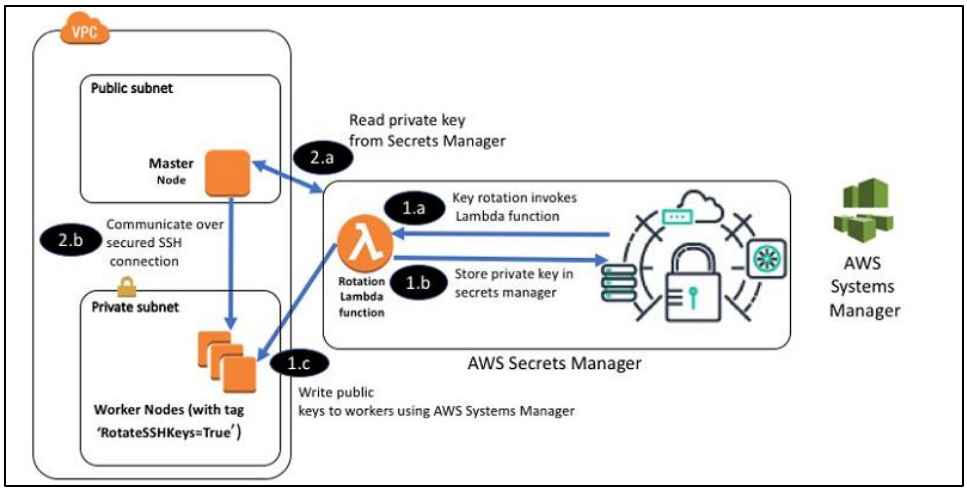

Figure 7: Key rotation flow

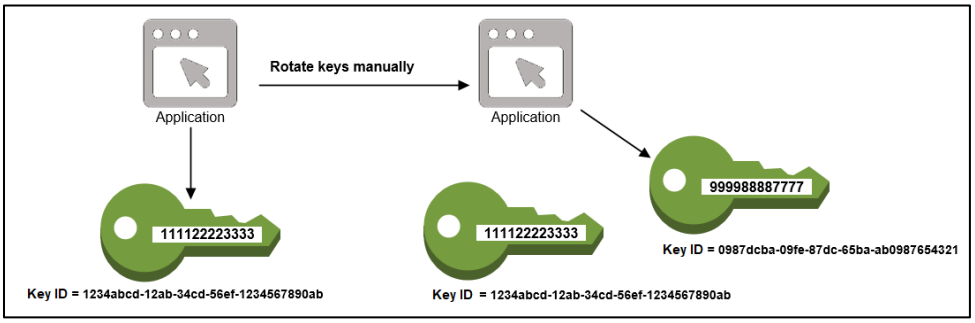

Figure 8: Example of key rotation

(a) Full Disk Encryption (FDE)

From the aspect of Theoretical Protection, Full Disk Encryption (FDE) ensures that all data on a hard disk or storage device is encrypted with a symmetric key *(Gillis, 2022)*. This means that even if the storage device is compromised or stolen, the data remains encrypted and cannot be accessed without the encryption key. With FDE, all files stored on Western Digital systems, including sensitive customer data, financial records, and intellectual property, are safeguarded against unwanted access and ransomware attack attempts by demanding authentication before the encryption key is provided. This prevents ALPHV, the unauthorized groups from booting the Western Digital system or accessing the data stored on the disk without proper authentication credentials. This adds an extra layer

of security. FDE stops attackers from accessing or altering the data even if they get remote access to the system by encrypting the entire disk. Furthermore, FDE has no effect on the data's accessibility to authorized users. After the user inputs the correct login credentials, the system makes the encryption key available and instantly decrypts the data, enabling users to view and interact with the data seamlessly.

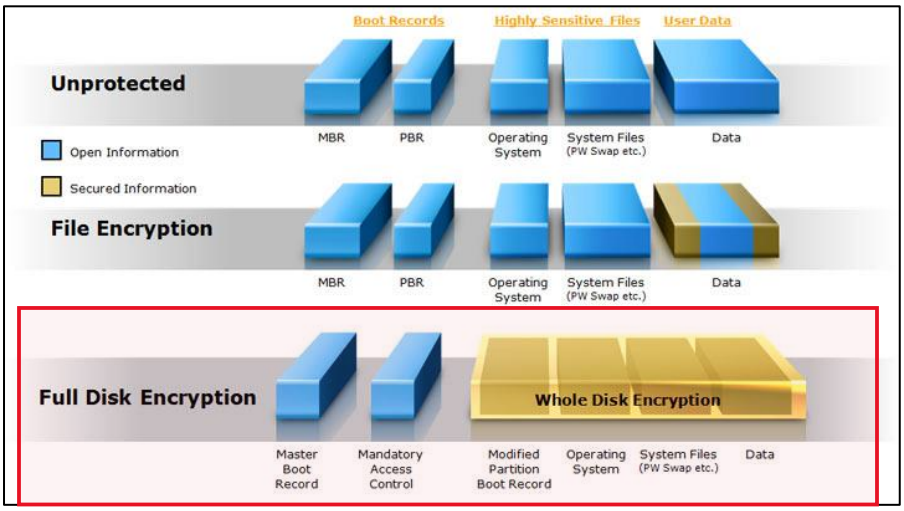

Figure 9: Full disk encrypted on Western Digital system.

For Practically Demonstration of Full Disk Encryption (FDE) Implementation at Western Digital, the first step needed is installation and configuration. To begin, Western Digital can ensure that all their computing devices, including workstations, laptops, and servers, are equipped with FDE capabilities. They can either choose devices that come pre-installed with FDE or deploy FDE software solutions compatible with their systems.

Figure 10: FDE application - the login screen for Checkpoint Endpoint

The entire disk or drive is automatically encrypted when FDE is configured. Strong encryption techniques like AES (Advanced Encryption Standard) are used to encrypt data in real-time as it is written to the disk. The encryption is transparent to the user, and they can continue using the system as usual.

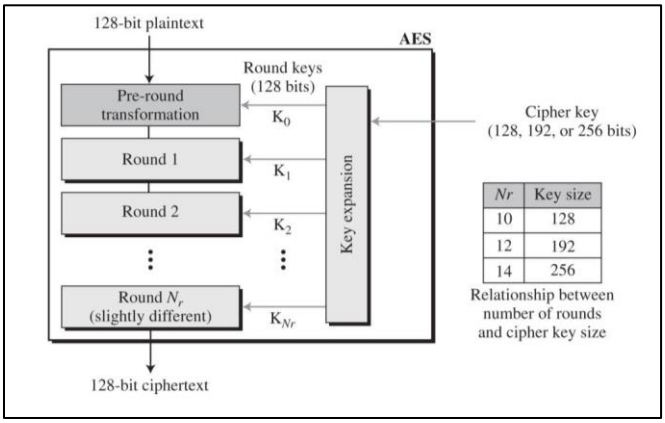

Figure 11: AES structure

When the system is powered on or the hard drive is accessed, the user is prompted to enter the required authentication credentials, such as a password, PIN, or biometric authentication. This authentication step is critical because it acts as a gatekeeper for access to the encryption key required for data decryption. Upon successful authentication, the encryption key is released, allowing the system to decrypt and access the data. By implementing strong authentication measures, Western Digital mitigates the risk of unauthorized users or malware bypassing the encryption and gaining access to the data.

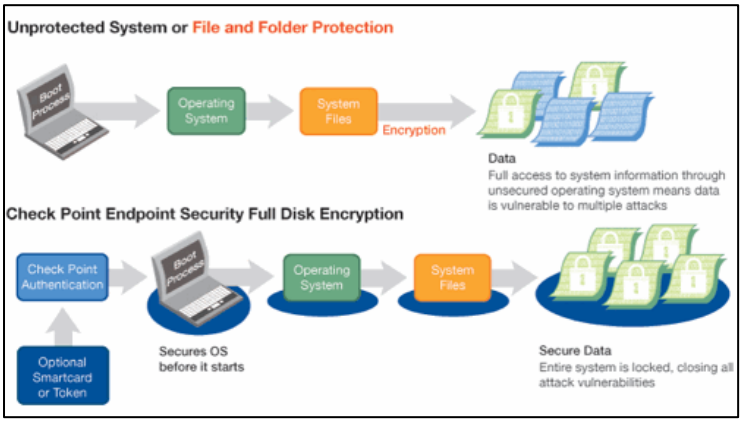

Figure 12: Full Disk Encryption locks the system down all the way to a pre-boot authentication.

Other than that, Western Digital will experience seamless data access once the user is authenticated. The system decrypts the data on the fly, allowing the operating system and applications to access and process the data as needed. Users can work with their files and applications without experiencing any significant performance impact.

In addition to protect data at rest, FDE provides a crucial layer of defense against ransomware attacks. Even if malware manages to infiltrate the system and attempts to encrypt the data, FDE renders the attack ineffective. Since the data is already encrypted, the ransomware cannot encrypt it again, thwarting the attacker's attempt to hold Western Digital's data hostage for ransom. This mitigates the potential financial and reputational impact of ransomware attacks, ensuring business continuity and customer trust.

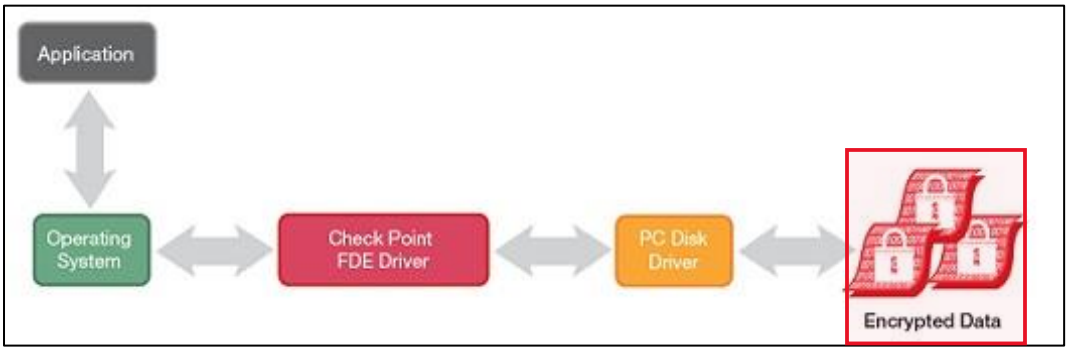

Figure 13: Flow chart of FDE

During the ransomware attack occurs, Western Digital can respond swiftly and effectively. By isolating the affected devices from the network, they can prevent further spread of the malware and minimize the potential damage. With proper incident response protocols in place, Western Digital can focus on removing the ransomware and restoring the encrypted data from secure backups. This rapid incident response strategy helps to minimize downtime, reduce data loss, and expedite the recovery process.

By embracing Full Disk Encryption, Western Digital demonstrates its commitment to data security and the protection of sensitive information. The practical implementation of FDE across their computing devices provides a robust defense against ransomware threats, ensuring the confidentiality, integrity, and availability (CIA) of their valuable data assets.

(b) Cloud Storage Encryption

From the perspective of Theoretical Protection, Western Digital can prevent unauthorized individuals, including hackers and malicious insiders, from accessing and reading sensitive information by encrypting the data before it is transmitted and while at rest *(Yang et al., 2020)*. Next, Cloud storage encryption allows Western Digital to segment and encrypt different data sets separately. This means that even if an attacker gains access to a portion of the encrypted data, he will not be able to access other data sets without the appropriate encryption keys. This segmentation provides an additional layer of protection that limits the potential impact of a data breach and ensures that the disclosure of one data set does not compromise the security of the entire storage infrastructure. In addition, Cloud storage encryption plays a vital role in mitigating insider threats, where employees or authorized personnel may attempt to access and misuse sensitive data. By encrypting data on the client side before it is uploaded to the cloud, Western Digital can ensure that only authorized individuals with access to the encryption keys can decrypt and view the data, regardless of their physical location or role within the organization.

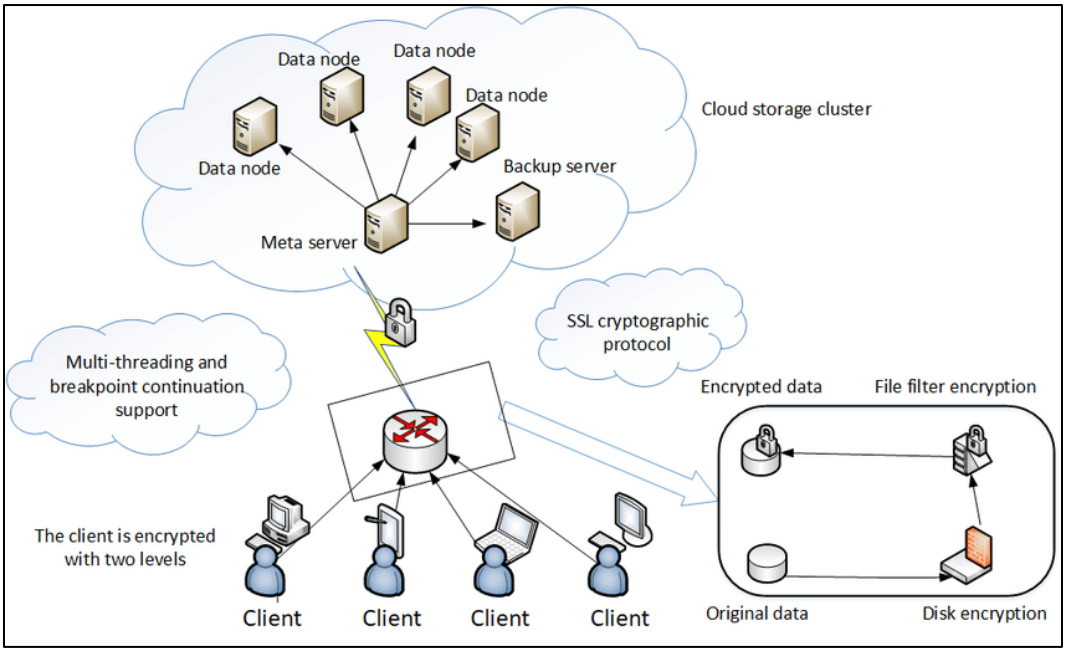

Figure 14: Cloud Storage System Architecture with Function of Encryption

In order to effectively implement cloud storage encryption through Practically Demonstration, Western Digital should begin by carefully evaluating and selecting a cloud storage provider that offers robust encryption capabilities. The chosen provider should support industry-standard encryption algorithms, possess a strong security record of accomplishment (track record), and provide transparent information about their encryption practices and key management procedures.

After a cloud storage provider is selected, Western Digital should carry out client-side encryption. This involves encrypting the data using their own encryption software or libraries before uploading it to the cloud. Client-side encryption ensures that the data remains encrypted during transit and at rest in Cloud storage. By retaining control over the encryption keys, Western Digital can maintain data privacy and ensure that the cloud storage provider does not have access to the plaintext data.

Additionally, Western Digital needs to establish secure key management practices. This involves generating encryption keys, securely storing them, and implementing proper key management procedures by Western Digital. Hardware Security Modules (HSMs), key management services, or other secure key storage mechanisms can be used to protect the encryption keys from unauthorized access and ensure their availability when needed for decryption.

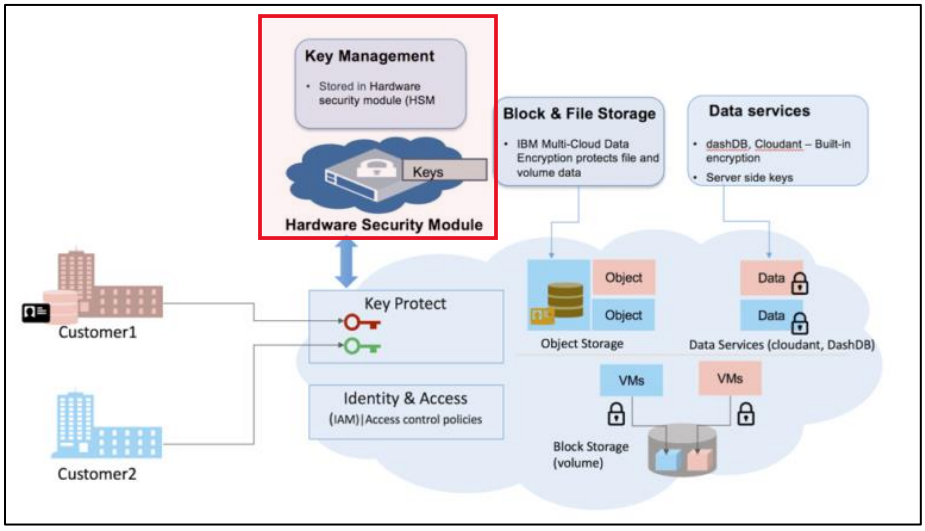

Figure 15: Encryption in Cloud storage - key management

When transferring data to and from Cloud storage, Western Digital should use secure communication protocols such as Transport Layer Security (TLS) or Secure Shell (SSH) to protect against eavesdropping and unauthorized access. TLS establishes a secure communication channel between the client and server. It ensures data privacy and integrity by encrypting the data in transit, preventing eavesdropping and unauthorized interception. Apart from that, SSH is another secure protocol commonly used for secure data transmission and remote system administration. It is suitable for transmitting sensitive information over untrusted networks.

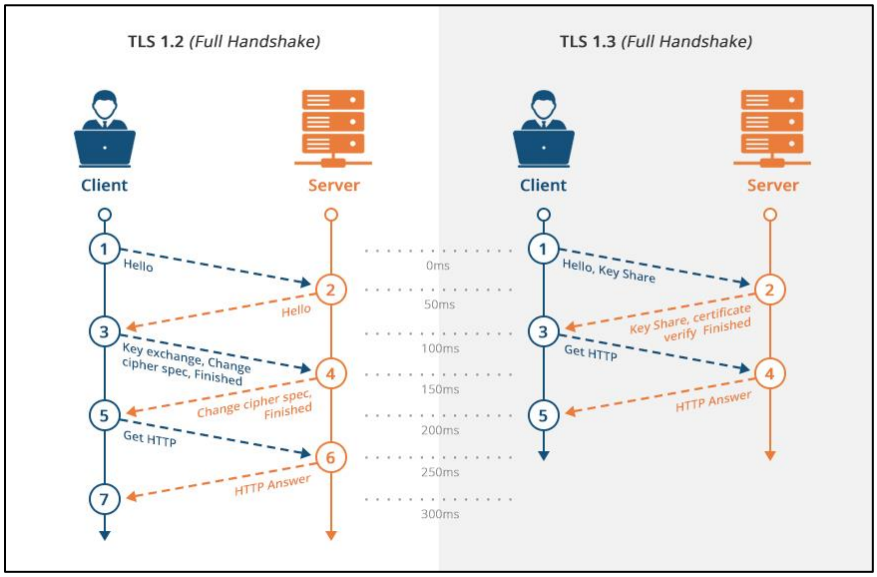

Figure 16: Transport Layer Security (TLS)

Moreover, Western Digital should implement strong access control mechanisms and authentication processes. This involves enforcing the use of strong passwords that are resistant to brute-force attacks and regularly reminding users to update their passwords. Multi-factor authentication (MFA) should also be implemented, requiring users to provide multiple forms of identification. Besides, it is important for Western Digital to conduct regular reviews of user access privileges. This involves regularly evaluating and updating user permissions based on their role and need for access to specific data.

By adopting these measures, Western Digital can safeguard its data from unauthorized access, reduce the risk of interception, prevent data breaches, and maintain control over its sensitive information stored in the cloud.

3.3.2 Message Authentication

Western Digital can incorporate message authentication techniques into its communication protocols and data storage systems. When transmitting sensitive data over networks, Western Digital can compute a MAC for the data using a shared secret key. This MAC is sent along with the encrypted data. When the encrypted data is received, the recipient can compute a new MAC using the same key and compare it to the received MAC. If they match, it means the data was not tampered with while in transit. For stored data, Western Digital can compute MACs for individual files or database records. Regular integrity checks can be performed by recalculating the MACs and comparing them with the stored values to identify any unauthorized modifications. Below are 3 main techniques that could utilize by Western Digital, which are:

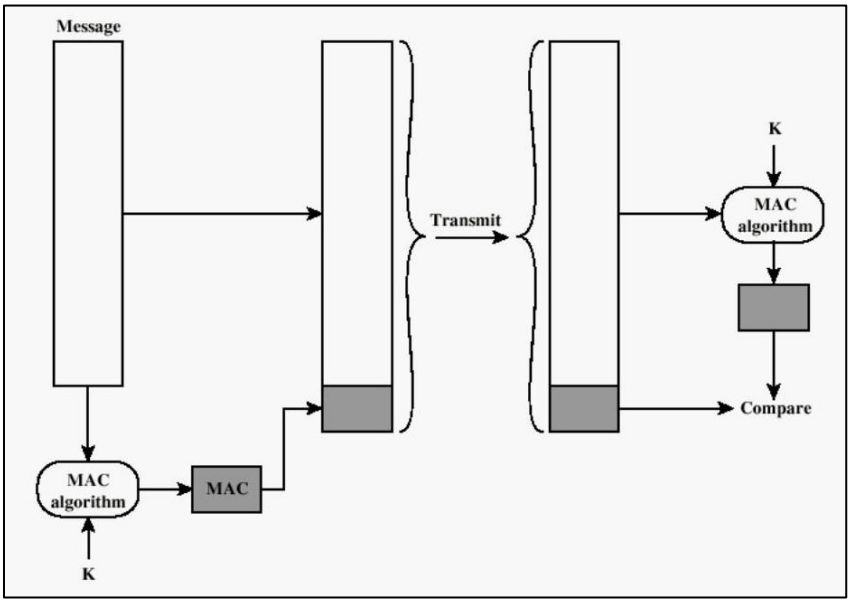

Figure 17: Message authentication using a message authentication code (MAC)

(a) Hash Functions

From the aspect of Theoretical Protection, Hash functions are mathematical algorithms that take an input message and produce a fixed-size hash value or digest *(Macharia, 2021)*. The resulting hash value is unique to the input data, meaning even a slight alteration in the input will produce a distinct hash value. This property makes hash functions ideal for data integrity checks. By comparing the calculated hash value of the received data to the original

hash value, Western Digital can verify the integrity of the data. If the hash values match, it means that the data has not been modified during transmission or storage. However, it is important to note that hash functions alone cannot guarantee authenticity or protect against unauthorized changes by attackers with knowledge of the hashing algorithm.

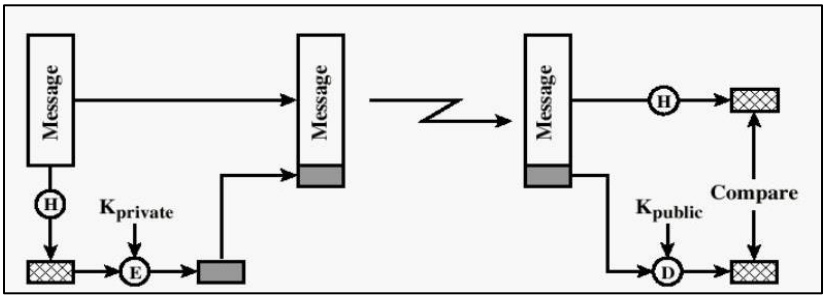

Figure 18: One-way hash function using public key encryption.

In order to practically demonstrate the use of hash functions for data integrity, Western Digital must first install and configure a reliable and widely used hash function, such as SHA-256, within their systems. This involves integrating the hash function into their software infrastructure or utilizing dedicated hardware components for faster computation. By following industry best practices and standards, Western Digital ensures that the implementation follows best practices and industry standards.

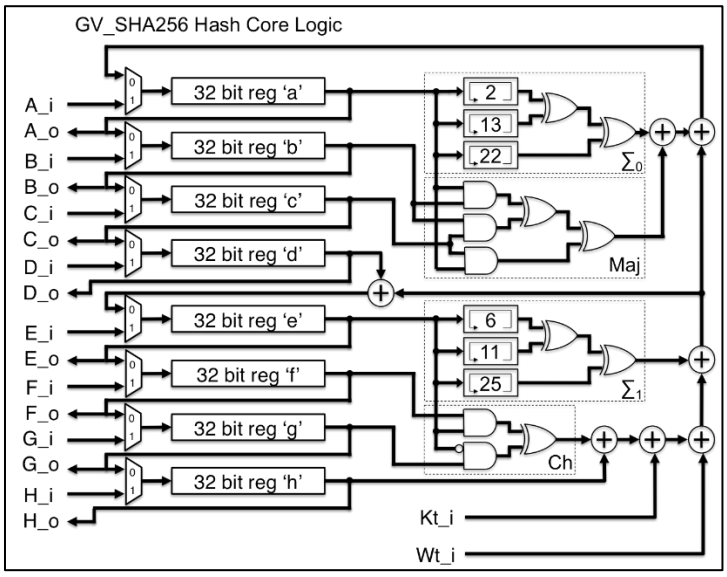

Figure 19: SHA-256 hash function

Once the hash function is in place, Western Digital can employ data integrity verification techniques. When Western Digital receives or retrieves a firmware update file, they compute the hash value of the data using SHA-256. This hash value serves as a fixed-size unique representation of the data. They compare this computed hash value with the original hash value stored or transmitted separately provided by the software provider. Through this method, Western Digital can determine whether the data has remained unchanged during its journey. If the computed hash value matches the original hash value, Western Digital can be confident that the firmware update file has not been tampered with during transmission or storage. In case of a mismatch, they can detect possible modifications or tampering, prompting Western Digital to take appropriate action to ensure the authenticity and integrity of the firmware update.

(b) Message Authentication Codes (MAC)

For Theoretical Protection, a Message Authentication Code (MAC) is a cryptographic technique that combines a secret key with the data to generate a tag or MAC value. MAC algorithms, such as HMAC or CMAC, utilize hash functions in their construction to ensure security and reliability *(Van & Thuc, 2015)*. Using a shared secret key, Western Digital can calculate the MAC value for their data. The recipient, possessing the same secret key, can verify the MAC value and ensure the integrity and authenticity of the received data. If the MAC values match, it indicates that the data is genuine and unaltered. MACs provide stronger protection than hash functions alone as they require a shared secret key to generate and verify the tag.

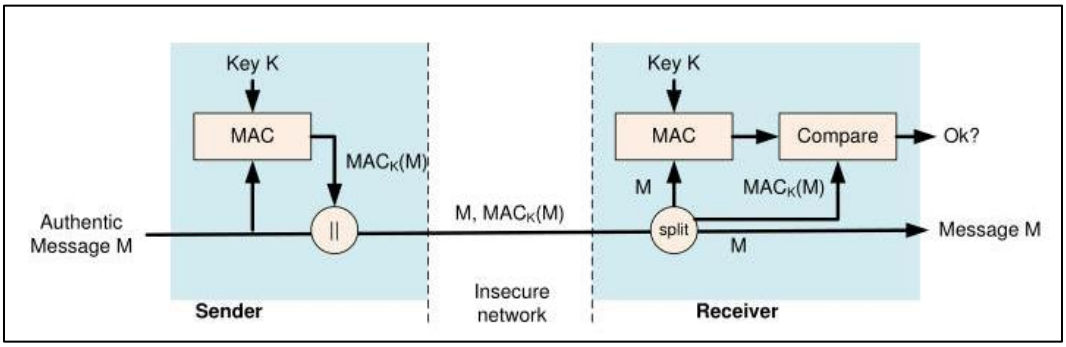

Figure 20: Flowchart of message authentication code (MAC)

To begin with the Practical Demonstration, the installation and configuration of a MAC algorithm, such as HMAC-SHA256, within Western Digital's systems is of utmost importance. They generate a secret key to be shared between the sender and recipient. It is imperative that the secret key is securely distributed and managed to prevent unauthorized access. Robust key management practices, including secure storage and controlled access, should be implemented to safeguard the confidentiality and integrity of the secret key.

Once the MAC algorithm is properly configured and the secret key is established, Western Digital can employ data integrity and authenticity verification techniques. Prior to transmitting data, the sender calculates the MAC value by combining the data with the secret key using HMAC-SHA256. This process generates a unique MAC value that serves as a digital fingerprint of the data.

During transferring the backup file to the remote server, the recipient possessing the same secret key verifies the MAC value upon receiving the data. If the MAC values match, it provides assurance to Western Digital that the backup file has not been modified during transmission. In the event of any discrepancies between the MAC values, it alerts Western Digital to potential modifications or tampering with the backup file, prompting appropriate action to ensure data integrity.

(c) Digital Signatures

From the perspective of Theoretical Protection, the sender signs the data using their private key, and the recipient can verify the signature using the corresponding public key. It refers to a cryptographic technique analogous to hand-written signatures. Western Digital can sign their data using algorithms such as Rivest–Shamir–Adleman (RSA) or Elliptic Curve Digital Signature Algorithm (ECDSA). The digital signature provides robust evidence that the data originates from the sender and has not been tampered with. For example. Western Digital acts as the sender digitally signs the document, establishing it is the document creator. While the client as the recipient can prove to someone that Western Digital and no one else (including WD) must have signed the document. Then, the recipient can verify the signature using Western Digital's public key. If the signature is valid, it ensures the integrity and authenticity of the data.

During the Practical Demonstration, Western Digital generates a key pair consisting of a private key and a corresponding public key using ECDSA. This algorithm provides robust cryptographic properties and is widely recognized in the industry for its security. The private key is generated in a secure environment and kept confidential, typically stored in a secure hardware device or a protected software key vault.

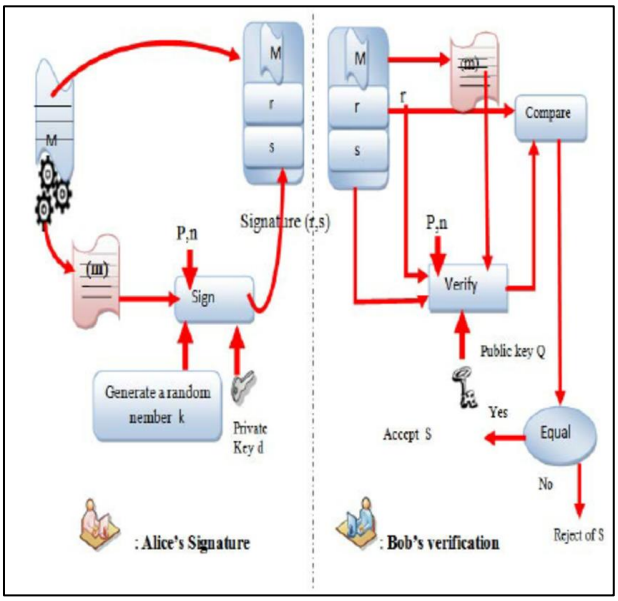

Figure 21:ECDSA signature and verification steps.

To ensure the integrity and authenticity of the public key, Western Digital follows best practices for key distribution. They may use digital certificates issued by trusted certificate authorities to bind the public key to a specific identity or entity. This helps establish trust and allows recipients to verify the authenticity of the public key when verifying digital signatures.

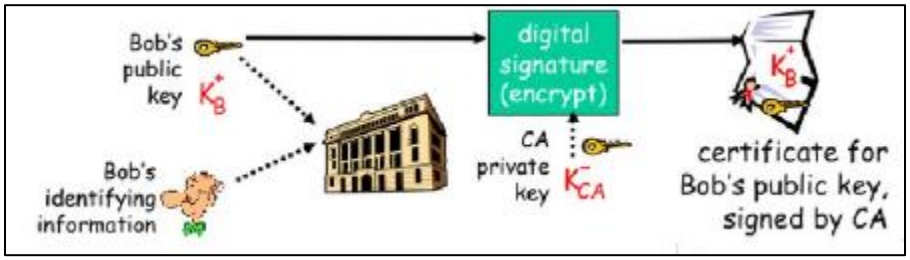

Figure 22: Role of certificate authority

Western Digital also implements proper key management practices to protect private keys from unauthorized access. This includes limiting access to the private key to only authorized personnel, implementing strong access controls, and regularly reviewing and updating key management procedures. They may use hardware security modules (HSMs) or other secure key storage mechanisms to safeguard the private key and prevent its compromise.

Additionally, Western Digital ensures that its digital signature implementation adheres to recognized standards and industry best practices. This includes implementing proper padding schemes to prevent known attacks and keeping up with any updates or patches to address emerging vulnerabilities. For example, when Western Digital wants to send a document or file, they sign it using their private key and create a digital signature. The recipient can verify the signature using Western Digital's public key. Next, they can also send contract documents to the client by signing the document using their private key. If the verification succeeds, the client can be confident that the document originated from Western Digital and has not been altered. Any modifications to the document would render the signature invalid.

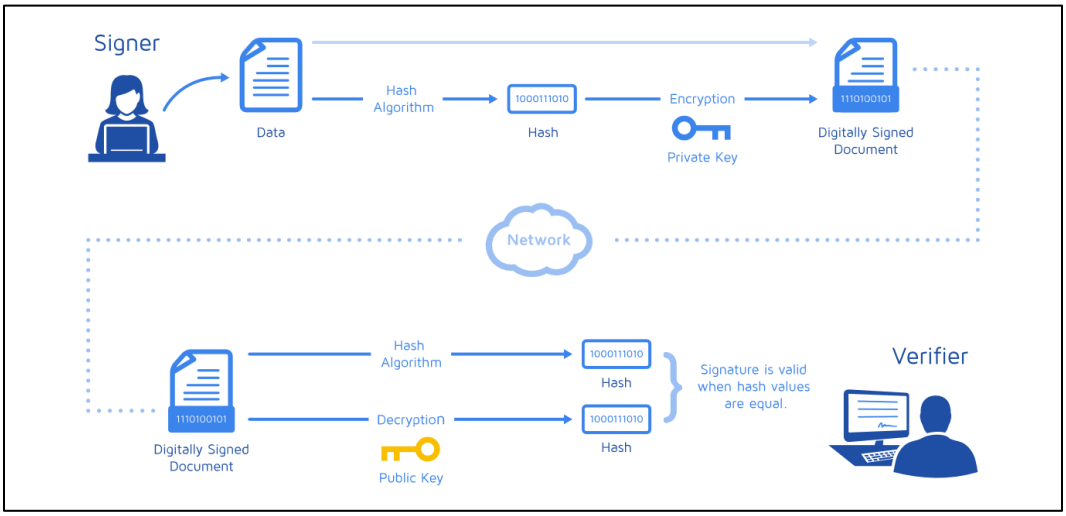

Figure 23: Process of digital Signing and verification

SECTION 4: CONCLUSION

This study sets out to present an analysis on the Western Digital Company security breach, identify the root causes of the attack, discuss the threat actor contributed, and explore how cryptographic techniques mitigate the breach, which ensures confidentiality, integrity, and availability (CIA) in the data.

In summary, the Western Digital security breach occurs due to a ransomware attack using web crawling on their system by the ALPHV group. Carrying out cryptographic techniques is a crucial step in addressing this barrier. The findings clearly identified 2 types of techniques, which are symmetric key encryption and message authentication according to the organization's current situation. Typically, cryptographic techniques act as a key factor in the company's security posture. Thus, these solutions not only alleviate the troubles but also increase the overall productivity of the Western Digital organization.

An implication of this study is the possibility that cryptography techniques should always be utilized as it plays a crucial role in handling the vulnerabilities in the system effectively. The analysis and research of the Western Digital ransomware attack security breach undertaken here successfully extended users, developers, and testing teams to carry out their checking, training, and updating operations on the platform systems to get the attack under control. To understand more clearly, I have concluded 3 main lessons learned from the Western Digital ransomware attack below:

- Implementing a defense-in-depth strategy combining multiple security measures.
- Importance of using strong encryption algorithms to protect sensitive data.
- Using secure cryptographic protocols with the latest advancements.

In a nutshell, some of the benefits of these findings are highlighted in this study. Cryptographic techniques for overcoming the ransomware attack and breach in the Western Digital company will be implemented appropriately in line with a piece of the system's ongoing development to satisfy evolving clients' demands. This enables the system to be continuously enhanced, as well as resolve any potential threats that may exist. Leaving the breach unsolved might have a major influence on overall production in the system and highly affect its users. Thus, it is necessary to explore the elimination of attacks earlier to build a more sustainable WD system. This would be a fruitful area for further work on studying machine learning and artificial intelligence techniques for ransomware detection and prevention.

REFERENCES

Chai, W. (2020). Western Digital Corporation (WDC). *WhatIs.com*. https://tinyurl.com/2htme6j7

Ciso, E. (2023, April 15). Hackers who stole 10TB Western Digital data, demand “8 figure” ransom. *ETCISO.in*. https://ciso.economictimes.indiatimes.com/news/data-breaches/hackers-steal-10tb-western-digital-data-demand-8-figure-ransom/99488363

Crane, C. (2023, March 20). *Symmetric Encryption 101: Definition, How It Works & When It’s Used*. Hashed Out by the SSL Store™. https://www.thesslstore.com/blog/symmetric-encryption-101-definition-how-it-works-when-its-used/

Cryptography Digital signatures. (n.d.). https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm

Gillis, A. S. (2022). full-disk encryption (FDE). *WhatIs.com*. https://www.techtarget.com/whatis/definition/full-disk-encryption-FDE

Ians. (2023, April 14). Hackers steal 10TB Western Digital data, demand ‘8 figure’ ransom. *Leaders Talk and Latest Tech News | CXO VOICE*. https://cxovoice.com/hackers-steal-10tb-western-digital-data-demand-8-figure-ransom/

Jefferson, B. (2023, March 16). *15 Common Types of Cyber Attacks and How to Mitigate Them*. Lepide Blog: A Guide to IT Security, Compliance and IT Operations. https://www.lepide.com/blog/the-15-most-common-types-of-cyber-attacks/

Macharia, W. (2021). Cryptographic Hash Functions. *ResearchGate*. https://www.researchgate.net/publication/351837904_Cryptographic_Hash_Functions

Mailangkay, M. D. a. R. M. F. M. B. A. (2023, April 19). *What is Data Encryption and Why is it Important*. School of Information Systems. https://sis.binus.ac.id/2023/04/19/what-is-data-encryption-and-why-is-it-important/

Malik, Z. (2021, October 18). 8 Benefits of Multi-Factor Authentication (MFA). *Ping Identity*. https://www.pingidentity.com/en/resources/blog/post/eight-benefits-mfa.html

Saw, R. (2023, April 14). *Hackers asking for 8-figure ransom after stealing 10TB of data from Western Digital - SoyaCincau*. SoyaCincau. https://soyacincau.com/2023/04/14/hackers-asking-for-8-figure-ransom-after-stealing-10tb-of-data-from-western-digital/

Staff, S. (2023a, May 3). Western Digital's ransomware response exposed by ALPHV ransomware. *SC Media*. https://www.scmagazine.com/brief/ransomware/western-digitals-ransomware-response-exposed-by-alphv-ransomware

Staff, S. (2023b, May 9). Western Digital: Customer data compromised in March attack. *SC Media*. https://www.scmagazine.com/brief/ransomware/western-digital-customer-data-compromised-in-march-attack

TechCrunch is part of the Yahoo family of brands. (2023, April 13). https://techcrunch.com/2023/04/13/hackers-claim-vast-access-to-western-digital-systems/

Techslang. (2021, January 20). What is Symmetric Encryption? *Techslang — Tech Explained in Simple Terms*. https://rb.gy/pkq1d

The Hacker News. (n.d.). *Western Digital Confirms Customer Data Stolen by Hackers in March Breach*. https://thehackernews.com/2023/05/western-digital-confirms-customer-data.html

Van, D. N., & Thuc, N. D. (2015). *A Privacy Preserving Message Authentication Code*. https://doi.org/10.1109/icitcs.2015.7292927

Waldman, A. (2023a, April 13). Western Digital restores service; attack details remain unclear. *Security*. https://www.techtarget.com/searchsecurity/news/365535041/Western-Digital-restores-service-attack-details-remain-unclear

Waldman, A. (2023b, May 8). Western Digital confirms ransomware actors stole customer data. *Security*. https://www.techtarget.com/searchsecurity/news/366537292/Western-Digital-confirms-ransomware-actors-stole-customer-data

Western Digital. (2018, February 28). Cleverism. https://www.cleverism.com/company/western-digital/

Western Digital - SG. (n.d.-a). *WDC-19009.* SanDisk and Western Digital SSD Dashboard Vulnerabilities | Western Digital. https://www.westerndigital.com/en-sg/support/product-security/wdc-19009-sandisk-and-western-digital-ssd-dashboard-vulnerabilities

Western Digital - US. (n.d.-a). *High-Performance SSDs, HDDs, USB Drives, & Memory Cards | Western Digital*. Western Digital. https://www.westerndigital.com/

Western Digital - US. (2023, May 5). *Western Digital Provides Update on Network Security Incident | Western Digital*. Western Digital. https://www.westerndigital.com/company/newsroom/press-releases/2023/2023-05-05-western-digital-provides-update-on-network-security-incident

Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. *IEEE Access*, *8*, 131723–131740. https://doi.org/10.1109/access.2020.3009876