Fortifying Cloud Security:
Advanced Models and Encryption
Strategies for Enterprises

Group Members

1. Cathy Zeng-Earnshaw
    - Student ID: 200324119
    - Brief Introduction: I am a database manager at the Ministry of Highways, leveraging my background in civil engineering alongside my passion for Computer Science. Pursuing my second degree in Computer Science, I am set to graduate in 2024 or early 2025. One of my standout courses has been cyber security, delving into vital aspects of data and database security, especially crucial as our data migrates towards cloud systems. This has triggered a personal interest in exploring Cloud Security.
2. Meet Devang Sevak
    - Student ID: 200433127
    - Brief Introduction: I am a final/senior year Bachelor of Computer Science student at the University of Regina with a forte in Software Engineering, Web Development and Cloud security. I am a Software Developer by profession, working at SGI Canada since April 2023 of this year, and I am also fascinated by cybersecurity and cloud security's role in the field of IT and Computer Science. My goal by the end of this course is to be prepared with good knowledge and understanding of cybersecurity and its important principles that I can apply anytime in my future career.
3. Krish Dharmesh Kumar Sheth
    - Student ID: 200445280
    - Brief Introduction: I am a third-year computer science student at the University of Regina with a personal interest in cybersecurity, software development, and networking. Throughout my academic journey, I have honed a keen interest in cybersecurity, particularly through a year-long internship at Nokia Canada, where I was actively engaged in software development and networking. I am committed to making a substantial contribution to the cybersecurity domain as I approach graduation in 2024. This research project has helped me dive deep into cryptography, various encryption algorithms, etc.

Fortifying Cloud Security: Advanced Models and Encryption Strategies for Enterprises

Abstract

Cloud computing has revolutionized the IT landscape, offering scalability, flexibility, and cost-efficiency. However, this transformation has brought forth complex security challenges. This paper explores the significance of cloud computing, focusing on cloud security concerns and encryption methods used in these environments. It analyzes ISO 270001's role, delves into IoT's integration with cloud security, and evaluates three advanced cloud security models: Chaos-Based Encryption & RBAC, ECSM-QKDP, and an Advanced Cloud Security Model. Each model's strengths, weaknesses, and implications for enterprise-level adoption are discussed. Based on enterprise needs and trade-offs between security, complexity, and resource demands, recommendations are provided.

Keywords**:** Cloud Security, Encryption Methods, Advanced Security Models

Introduce the significance of cloud computing and the challenges associated with cloud security

Cloud computing is the on-demand availability of computer (Adam, 2020) systems resources on remote servers hosted on the internet. It is vital to reshape modern IT landscapes, offering scalability, adaptability, and cost-effectiveness across industries. Cloud computing offers three primary service models – infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) – each catering to specific needs and providing varying levels of abstraction and flexibility for businesses seeking efficient cloud solutions. IaaS offers scalable computing resources without direct hardware purchase, such as Amazon Web services (AWS) and Microsoft Azure. In contrast, PaaS, such as Goole App Engine and Heroku, focuses on providing cloud components for applications, leaving infrastructure management to the provider. The most prevalent SaaS, such as Salesforce and Google Workspace, deliver cloud-hosted services directly via the Internet, reducing the need for client-side downloads or installations and offering user-friendly accessibility (Adee & Mouratidis, 2022). This technological revolution brings forth multifaceted challenges, prominently in security. As organizations migrate their sensitive data to cloud environments, concerns regarding unauthorized access, data breaches, and privacy violations become paramount. The collaborative security model, where cloud service providers and users share responsibility for security, introduces complexities and potential vulnerabilities. Furthermore, the dynamic nature of cloud services, characterized by continual updates and modifications, necessitates a forward-thinking and adaptable security approach to safeguard data integrity, confidentiality, and accessibility within the cloud. (Erl & Barcelo Monroy, 2023)

Cloud Security Concerns

Cloud security concerns encompass a spectrum of issues due to the unique characteristics of cloud computing. (Khan, 2009) Unauthorized access and data breaches pose significant risks as shared infrastructure in cloud environments raises vulnerabilities. Effective authentication mechanisms and robust access controls are essential to mitigate these risks. Additionally, compliance with regulations like GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), or PCI DSS (Payment Card Industry Data Security Standard) (Bermejo-Gil, 2021) within cloud environments requires collaboration between service providers and users to ensure adherence, failure of which could lead to legal and reputational repercussions. The ever-changing nature of cloud services presents further security challenges, requiring proactive management to address potential vulnerabilities. Data protection, encryption, and managing privacy concerns in distributed data storage across different geographical locations are critical aspects of cloud security. (Adee & Mouratidis, 2022)

Internet of Things (IoT) and Cloud Security

The Internet of Things (IoT), the network of smart devices that communicate through the internet, has gotten a lot of attention in these modern days. This is because the growth in this technology has resulted in large amounts of data being produced. Cloud computing makes it possible for users of IoT devices to store and process data generated by IoT at an affordable cost. The cloud acts as a conduit through which IoT processes flow and allows collaboration with other developers. The open nature of the IoT cloud ecosystem makes it simple for users to add new IoT devices within their reach. These systems utilize public HTTP as a means of communicating with the cloud. However, major security challenges arise from the

inclusivity of many connected devices from various users and manufacturers through an IoT hub. This large-scale IoT cloud system demands an effective, flexible security framework that maintains information sovereignty and authenticity. Moreover, in an IoT cloud system, people are more actively involved. The system collects data from human activities and provides a platform for users to control IoT devices. Consider a device that can be used by different people, each with unique use patterns. This increased human interaction also introduces new potential points of attack to the security framework. (Chen, Luo, & Xiang, 2021)

ISO 27001 and Cloud Security

The ISO 270001 standard is a globally recognized information security management system (ISMS) specification. ISO 27001 provides a systematic approach to managing sensitive company information, ensuring it remains secure. This standard outlines requirements for establishing, implementing, maintaining, and continually improving an information security management system. (ISO 27001 Compliance Services) It helps organizations identify potential risks to their information security and puts in place controls and measures to manage and mitigate these risks effectively. ISO 27001 covers various aspects of information security, including risk management, access control, encryption, security policies and procedures, incident management, business continuity planning, and compliance. Compliance with ISO 27001 demonstrates to stakeholders, clients, and partners that an organization takes information security seriously and has measures to protect sensitive data. Integrating ISO 270001 standards into the cloud services models is imperative for fortifying cloud security and ensuring compliance with internationally recognized security practices.

Encryption Method used in cloud computing

According to Adee and Mouratidis**,** different encryption methods are used in cloud computing; here is the comparison table outlining each method.

Encryption Method	**Description**	**Use Case**	**Kay Management**	**Performance Impact**
Symmetric Encryption	Use a single key for both encryption and decryption	Data storage, fast and efficient encryption	Key distribution is critical	Low impact, faster processing
Asymmetric Encryption	Utilizes a pair of keys (public and private)	Secure data transmission, key exchange	Management of public and private keys	Slower due to complex mathematical operations
Homomorphic Encryption	Allows computations on encrypted data without decryption	Secure computations in the cloud, privacy-preserving	Complex key management, limited practical implementations	Significant computational overheads
Quantum Cryptography	Leverages principles of quantum mechanics for encryption	Protects data against future quantum computer threats	Requires quantum-safe algorithms in the developmental stage	Potentially high performance, quantum-resistant
Attribute-Based Encryption	Access control based on attributes of users	Fine-grained access control, data sharing	Key management tied to user attributes	Depending on the implementation, overheads vary
Proxy Re-Encryption	Allows a third party to alter the encryption	Delegated access, secure data sharing	Involves a proxy re-encryption key, complex management	Moderate impact depending on the re-encryption process

Table 1: Cloud Computing Encryption Methods Comparison Table

Each encryption method has its strengths and weaknesses, catering to different use cases and security requirements in cloud computing, key management, performance impacts, and the specific use case heavily influence the choice of encryption method in a cloud environment. In Adee and Mouratidis' research, they have mentioned the cloud computing security model, only employing encryption algorithms in data storage and transmission which is insufficient due to the following reasons:

1. **Key Vulnerabilities:** Encryption heavily relies on key management. If encryption keys are compromised or mismanaged, it can lead to data breaches. In cloud computing, managing keys securely becomes challenging due to the shared responsibility model between the cloud provider and the user.
2. **Access Controls:** Encryption protects data from unauthorized access, but access control becomes crucial once data is encrypted. Ensuring proper access controls and monitoring user actions post-decryption in cloud environments is equally important.
3. **Insider Access:** Encryption doesn't prevent authorized users from accessing and potentially misusing sensitive data. Cloud environments often have multiple users with varying access levels, posing a challenge in monitoring and preventing insider threats.
4. **Dependency on Providers:** Encryption helps protect data from unauthorized access; in many cases, cloud providers retain some control over encryption keys or the encryption processes, creating potential vulnerabilities if the provider's security measures are compromised.

Due to the insufficiency of encryption in the cloud environment, a combination approach for the cloud security model may need to be considered to improve access controls and data security within a cloud environment.

Data Security

Data security is a method for implementing the preservation and shielding of important data and information stored and used in digital format from unauthorized access and personnel who can cause damage, leaks, and threats to the whole process. It takes care of all elements of data security,

whether it be hardware components such as memory storage drives for storing data or software for having admin privileges and various other applications for security. (What is data security?)

Different Types of Data Security

Method of Encryption: With this method, data or information such as texts and strings can be converted into Ciphertext or an encrypted form, making it hard for an unauthorized person to figure out the text. Authentic specified users typically use encryption keys for accessing data or files. In some cases, there's also tokens available for a large number of users and data.

Masking of Data: Data is often masked for businesses to create software or in-house apps for training purposes by making use of real insights. The goal here is to hide private and sensitive data as much as possible.

Data Deletion: This is a much more protected and reliable mechanism for clearing and cleaning data, which ensures that data is wiped off from a Data source or Memory Storage. Its main goal is to ensure that one cannot recover data at any cost but permanently delete it.

Data Flexibility: If an incident occurs in a company regarding data outage or power failure, this is resolved by monitoring how easily the company can regain its strength from incidents that hampered the organization's data. A quick and easy recuperation is required for a company to reduce the amount of damage caused to the data.

How is Data Security related to Cloud Data Security?

Data Security is as important to understand as Cloud Security because it plays a major role in including its elements for protecting data over the cloud platform. The term is known as Cloud data Security, a technique in which a cloud service provider provides us with different technological tools, functionalities and controls for preserving any secure data stored in a cloud in abundance from data leaks, data abuse, piracy of information, etc. Cloud platforms sometimes incorporate all the Data mentioned above to enhance the security of information stored on the cloud. A cloud data security protocol protects three kinds of data or information:

- **Data getting utilized:** Protection of data that is getting utilized by in-house software, apps, database systems or even via validating user accesses (for example, Multi-Factor Authentication systems)
- **Data getting Transmitted:** Monitoring and ensuring that the private information and important data doesn't get hampered and its integrity remains constant throughout transfer and data exchange.
- **Data that got stored:** Preservation of data and vital information saved on the cloud environment. User accounts of the cloud should have validated access for all cloud applications and network drives located on local machines (Alvarenga, 2022).

Nowadays, storing data and information on the cloud is way more versatile than one ever thought. A few Reasons why a business organization would prefer cloud data storage more for protecting data are:

- **Cost-Efficient:** It is pocket-friendly for most companies as the framework of data storage and cloud data security tools is priced amongst multiple employees.

- **Maintenance:** Optimizing the Cloud environment, making changes according to a business and maintaining it is all managed by the service provider which technically drops down to lower estimated cost.
- **Better Access Options:** Data can be accessed by any authorized and authenticated personnel from any machine or place in the world with the help of a network (Alvarenga, 2022).

Research Goal and Objectives of this paper

This research paper will focus on scanning and evaluating different advanced cloud security models that enhance data security and maintain privacy in cloud computing environments. (Mouratidis & Mouratidis, 2022)To achieve the research objectives, the first is to research the existing cloud security models that apply a combination of encryption and another (Jose & Victor, 2020) method. Three advanced models are summarized in the next portion of this report.

Enhanced Cloud Security Models

Chaos-Based Encryption & RBAC models:

A comprehensive cloud security model with Enhanced Key Management, Access Control and Data Anonymization Features has been proposed by Mini and Viji to resolve the rising cloud security issues. (Mini & Viji, 2017).

Mini and Viji's model the following components:

- Data Owner (DO) owns the data and provides cloud storage or processing services.;

- Cloud Service Provider (CSP), which is a third-party service provider storing data, such as Microsoft Azure or Amazon Web Services (AWS);
- Key Management Module (KM), which is responsible for key generation and sharing between DO and Data User (DU);
- Data User (DU): individuals or entities accessing data stored in the cloud.
- Transmission Space (TS): unsecured channel used for data transmission.

Security Features that are used in the model include:

- Chaos-Based Encryption: Utilizes chaos theory for key generation to enhance security against attacks.
- Flexible Access Control: implements role-based access control (RBAC) for user data sharing.
- Data Anonymization: masks data before transmission to unregistered users for enhanced privacy.
- Trust Modules: monitors user behaviour, enforces access privileges, and enables emergency access.

For this model, the DO encrypts data using chaos-based key generation before transmitting it through TS to CSP. Alongside data transmission, access structures and roles are sent to CSP for RBAC implementation. CSP stores encrypted data, implements RBAC and data masking, and runs a trust module. Trust Module dynamically monitors user behaviour, enforces access privileges, and facilitates emergency access. KM shares DO's ID with DU for authentication and facilitates double encryption/decryption for data access. This model has a few advantages: it enhances security and chaos-based encryption highly resists various attacks. Flexible access control: The RBAC allows granular control over data access based on roles. Dynamic Trust Management monitors user behaviour for trust enforcement and emergency access. Data

Privacy: Anonymization ensures user privacy by masking data for unregistered users. Emergency access provision enables secure data access in critical situations through proper authentication.

This model also has a few disadvantages: it is a complex system involving multiple modules and processes, which can increase complexity. High resource requirements, running separate modules (KM, Trust Module) might require additional computational resources. It could lead to maintenance challenges, as managing and updating the system components might pose maintenance challenges. Last dependence on key management, if the key management system is compromised, it could lead to security vulnerabilities. In summary of Mini and Viji's proposed model, the infrastructure aims to provide a robust security framework for cloud computing. Still, its complexity and resource requirements could pose challenges in implementation and maintenance at the enterprise level, leading to a failure in the practical world.

ECSM-QKDP Model:

Sundar, Sasikumar and Jayakumar proposed another cloud security model using QKDP (ECSM-QKDP) for more advanced data security over the cloud. (Sundar, Sasikumar, & Jayakumar, 2022). The proposed model aimed to enhance the security of communication between the cloud server (CS), data owner (DO), and legitimate user (LU) within a cloud environment. It operates through various phases that involve initial preparation, communication measurement, BB84 QKDP Framing, and a secure authentication protocol (SAP) comprising distance bounding and HASBE-based key generation. The workflow in this model involves matrix-based preparations by DO and transmission of qubits to CS. DO derives information and selects qubits for transmission to CS. It utilizes the BB84 protocol for secure quantum key distribution and employs SAP for secure authentication. Secure Authentication Protocol (SAP) encompasses distance binding and HASBE-based key generation. The distance bounding ensures

secure transmission by verifying round trip time and encrypted content. HASBE-based key generation utilizes attributes and a security factor for generating secure keys and encryption processes.

The advantages of this model are that it leverages quantum properties for enhanced security in key distribution; It uses distance bounding to help prevent relay attacks and ensure secure data transmission; It utilizes encryption processes such as HASBE for secure data sharing and decryption, which has proven this model is highly secure. However, there are disadvantages to this model as it involves quantum-based protocols and encryption mechanisms, which might be challenging to implement and maintain. It is also resource intensive, like Mini and Viji's model, as the Quantum-based security protocols often demand significant computational resources. Also, it requires specialized knowledge and expertise in quantum computing and cryptography for implementation and maintenance.

In summary of Sundar, Sasikumar and Jayakumar's model, the ECSM-QKDP presents a forward-looking approach to cloud security by incorporating quantum-based protocols, enhancing data confidentiality, and ensuring secure communication. However, its complexity and resource-intensive nature might pose widespread adoption and implementation challenges. The efforts towards amplification and resource optimization would be vital to make this advanced security model more accessible and applicable to a broader range of cloud computing scenarios.

Advanced Cloud Security Model:

The third model used in the research is Jose and Victor's security-enhanced model for cloud data based on dynamic data fragmentation and replication. (Jose & Victor, 2020). This model aims to enhance data availability and confidentiality during data file outsourcing. It comprises several key components:

1. AES encryption: Utilizes the Advanced Encryption Standard (AES) algorithm with 128-bit clocks and keys for data encryption.
2. Dynamic Fragmentation: Fragment data files based on runtime feedback of available virtual machines to enhance security against node-level attacks.
3. Replication: replicates across different cloud notes to ensure high availability and accessibility.

The advantages of this model are that it enhances security like the two other modes. The AES encryption and dynamic fragmentation contribute to heightened data security. It also has disadvantages; for example, the complexity of this model is comparable to the two other models due to the involvement of encryption fragmentation and replication mechanisms. It also requires significant computational resources and sophisticated infrastructures; redundancy management is involved in handling and deleting redundant replicas, which could be challenging and require further development.

To compare these three models at an enterprise level:

ECSM-QKDP model emphasizes quantum-based security protocols for communication between cloud entities, ensuring high-level encryption and authentication. It is complex to implement and requires specialized knowledge.

Chaos-Based Encryption & RBAC focuses on chaos-based encryption, role-based access control, and trust management for cloud data security. It offers flexibility and resilience against attacks but might demand computational resources.

Advanced Cloud Security Model integrates AES encryption, dynamic fragmentation, and replication to enhance data security and availability. Balance security and availability efficiently but might pose implementation complexity.

Recommendations

From an enterprise perspective, traditional models show vulnerabilities, prompting the need for a comprehensive solution. Therefore, our proposed model/solution not only responds to the vulnerabilities and limitations of current cloud security models but provides an advanced way of integrating artificial intelligence (AI) with already established cybersecurity methods. This innovative approach will improve the agility and flexibility of the security framework, overcoming barriers associated with conventional encryption techniques. The major components of the proposed model are:

Specialized Key Management System (SKMS):

The system consists of an AI-powered key generation system that will use machine learning algorithms that evaluate historical data, users' personal habits, and contextual information for the development of dynamic encryption keys in a real-time manner. The system constantly learns and adapts with its keys to avoid static keys which would be prone to vulnerabilities. The dynamically generated key in this regard diminishes the risk of static key infrastructure, providing room for a more adaptable and safe cloud setting. SKMS will also play an important role in key distribution, which is tied to the user's roles, tasks and data sensitivity. This means that the cloud security architecture becomes more resilient as there is a correlation between the user and data security requirements.

AI-Powered Behavioral Analysis and Anomaly Detection:

Machine learning adoption in user behaviour analysis increases safety and makes a cloud operation system more efficient. The system should be able to understand what is considered normal behaviour in the system, and any deviations will promptly be detected, which may imply potential security breaches. This especially provides a solution to attacks within an organization, such as insider attacks. Moreover,

there would be a response system which would involve incorporating AI-based anomaly detection and real-time response mechanisms. The system would automatically initiate incident-control security protocols and enforce restrictions like implying access limits or adding extra layers of authentication to protect cloud service availability and integrity after detecting peculiarities.

Adaptive Access Control through AI:

The system uses machine learning algorithms to predict an access requirement based on past user behaviour, roles and responsibilities. The predictive model ensures that users receive only necessary access privileges, reducing the chances of exposing unauthorized data. Additionally, the AI-driven access control system can adjust its access controls based on user interaction. The security framework is updated regularly, enabling it to adapt to the changing environment and threat landscapes of the organization.

AI-Driven Threat Intelligence:

The cloud becomes a proactive defense environment using AI-enabled threat intelligence systems. Through threat intelligence, machine learning algorithms can help predict possible cybersecurity attacks. The system identifies possible vulnerabilities and takes corrective actions, such as changing crypto-graphic protocols and strengthening physical access control in a bid to contain the potential risk of compromise.

Cryptographic Methods:

Advanced Encryption Standard (AES) forms a major part of our security model to offer strong encryption for data storage and transmission. The use of this symmetric encryption algorithm has become worldwide due to its ability to generate high performance, strength and resilience against vulnerabilities that are known. Symmetric encryption algorithm involves utilizing the same key for encrypting and

decrypting. Nevertheless, as opposed to ours, the conception of how dynamic keys are generated, distributed, and updated on a regular basis is assisted via artificial intelligence (AI) technology. It is an AI component that keeps track of different things, such as user behaviour, current threats, etc. The use of machine learning algorithms enables the AI system to identify trends and patterns in the data and detect changes or abnormalities in user behaviour or security threats. The AI dynamically generates new symmetric encryption keys based on the insights gained through continuous monitoring and analysis. This ensures that the encryption process is not reliant on static keys and can adapt to changes in the security environment. After generating new keys with this AI-driven key management system, the cryptographic strategies are matched to individual users' roles with respect to the sensitive nature of the data being stored as well as the overall security needs of the cloud environment. The AI regularly updates the encryption keys to ensure that one is not used for a long period, minimizing the impact of potential compromises. While AES remains a symmetric encryption algorithm, the dynamic key management system driven by AI introduces a level of adaptability and responsiveness to the encryption process. This approach ensures that even within the constraints of symmetric cryptography, the model can dynamically adjust encryption keys based on real-time insights and evolving security requirements, enhancing the overall robustness of the cloud security framework.

Steganography for Advanced Protection:

Integrating steganography adds another level of encryption that improves the existing cryptographic security and secrecy attributes of cloud-based stored data. This enhancement goes beyond traditional encryption, safeguarding data even in the event of a compromise.

Continuous Learning and Evolution:

The adaptable nature of cloud services is greatly enhanced by our AI-driven security solution's ongoing learning and evolution. The system's algorithms are constantly improved by considering security incidents, new threats, and real-world experiences. The AI recognizes possible threats and initiates proactive actions by means of real-time threat monitoring, pattern recognition, and anomaly detection. The system incorporates the most recent threat intelligence data, modifies access control settings, and advances its understanding of user behaviour. This dynamic procedure keeps up with new dangers and promotes an adaptable cloud environment to guarantee a robust and responsive security framework.

Conclusion

Cloud computing presents an innovative paradigm in IT, but security remains a pivotal concern. Understanding the multifaceted challenges associated with cloud security, especially regarding encryption methods and advanced security models, is critical for organizations. The evaluated models offer diverse approaches to fortify cloud security, but each has complexities and resource implications. Chaos-Based Encryption & RBAC stands out due to its alignment with existing enterprise systems, emphasizing a blend of encryption and access control. However, a comprehensive evaluation based on specific organizational requirements and security trade-offs is imperative. The proposed cloud security model, with its integration of AI, not only addresses existing vulnerabilities but transforms the cloud computing environment into a resilient, intelligent, and efficient ecosystem. It brings about a paradigm change in the cloud infrastructure by emphasizing proactive security, reducing interruptions, maximizing resource usage, and encouraging a continuous improvement culture.

References

Adam, G. P. (2020). COTS-Based Architectural Framework for Reliable Real-Time Control Applications in Manufacturing. *Applied Sciences*, 3228.

Adee, R., & Mouratidis, H. (2022). Dynamic Four-Step Data Security Model for Data in Cloud. *Sensors*.

Alvarenga, G. (2022). CLOUD DATA SECURITY:. *Crowdstrike*. Retrieved from https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-data-security/

Bermejo-Gil, B. P.-R.-R.-M.-R. (2021). RespiraConNosotros: A Viable Home-Based Telerehabilitation System for Respiratory Patients. *Sensors*.

Chen, F., Luo, D., & Xiang, T. (2021). IoT Cloud Security Review: A Case Study Approach Using Emerging Consumer-Oriented Application. *ACM Comput*, 36. doi:https://doi.org/10.1145/3447625

Erl, T., & Barcelo Monroy, E. (2023). *Cloud Computing: Concepts, Technology, Security, and Architecture, 2nd Edition.* The Pearson.

ISO 27001 Compliance Services. (n.d.). *Integris*. Retrieved from https://integrisit.com/services/compliance/iso-27001/

Jose, P., & Victor, S. (2020). Security Enhanced Model for Cloud Data Based on Dynamic Data Fragmentation and Replication (DDFR). *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 766-771.

Khan, K. M. (2009). Security Dynamics of Cloud Computing.

Mini, G., & Viji, K. (2017). A Comprehensive Cloud Security Model with. *International Journal of Communication Networks and Information Security (IJCNIS)*, 263.

Mouratidis, H., & Mouratidis, H. (2022). A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography. *Sensors*.

Roesler, V. B. (2022). Special Topics in Multimedia, IoT and Web Technologies.

Sundar, K., Sasikumar, S., & Jayakumar, C. (2022). Enhanced cloud security model using QKDP (ECSM-QKDP) for advanced data security over cloud. *Quantum Information Processing*.

What is data security? (n.d.). Retrieved from https://www.ibm.com/topics/data-security