



Tribhuvan University

Faculty of Humanities and Social Science

**A FIELD VISIT REPORT ON
GOVERNMENT INTEGRATED DATA CENTER (GIDC)**

Submitted To

Department of Information Technology

Kathford International College of Engineering and Management

In Partial Fulfilment of the Requirements for the Bachelor of Computer Application

Submitted By

Khemraj Bahadur Raut(6-2-456-58-2022)

Submitted To

Ms. Sarita Neupane

July 2026

ACKNOWLEDGEMENT

We would like to extend our heartfelt gratitude to **Mr. Mukesh Kushwaha**, Computer Operator in the Information Technology Department at the Government Integrated Data Center, Singha Durbar, for generously taking time out of his busy schedule to guide us through the server rooms. His detailed explanations, patience, and willingness to answer all of our questions made the visit both informative and engaging. His insights gave us a much better understanding of how a modern government data center operates.

We would also like to sincerely thank the other staff members at the Government Integrated Data Center for their warm hospitality and valuable assistance throughout the visit. Whether it was explaining the purpose of a particular system or guiding us through different sections of the facility, their support greatly enriched our learning experience.

Finally, we express our deepest appreciation to **Ms. Sarita Neupane**, faculty member at Kathford International College of Engineering & Management, whose dedication and continuous efforts made this educational visit possible. From arranging the visit passes to coordinating with the Singha Durbar administration for entry and security clearance, she handled every detail with great care and professionalism. Without her initiative, guidance, and commitment, this valuable learning opportunity would not have been possible.

TABLE OF CONTENTS

ACKNOWLEDGEMENT	i
TABLE OF CONTENTS	ii
CHAPTER 1: INTRODUCTION	1
CHAPTER 2: OBJECTIVES	3
CHAPTER 3: FIELD OBSERVATION	4
3.1 Infrastructure Used.....	4
3.2 Services Provided.....	7
3.3 Security Measures	9
3.4 Disaster Recovery Plan.....	10
3.5 Backup and Recovery	12
3.6 Future Plans	13
CHAPTER 4: LEARNINGS.....	16
CHAPTER 5: CONCLUSION.....	18
REFERENCES	19
APPENDIXES	20

CHAPTER 1: INTRODUCTION

The **Integrated Data Management Center (IDMC)** is a government organization operating under the **Department of Information Technology (DoIT), Office of the Prime Minister and Council of Ministers, Government of Nepal**. It serves as the country's central facility for providing secure, reliable, and modern IT infrastructure that supports digital governance and the delivery of public services across government agencies. The official website, <https://idmc.gov.np>, serves as the primary source of information about the center's services, resources, notices, publications, and ongoing digital initiatives.

The main objective of IDMC is to strengthen Nepal's digital transformation by providing robust IT infrastructure, centralized data management, and secure e-Governance solutions. The center envisions becoming a leading force in digital transformation by delivering efficient, transparent, and citizen-focused public services. Its mission is to empower government institutions through secure data management, advanced computing infrastructure, and innovative digital technologies while ensuring the protection and availability of critical government information.

To support government organizations, IDMC offers a wide range of essential services, including domain registration, internet connectivity, Virtual Machine (VM) and Virtual Private Server (VPS) hosting, server colocation, data backup and disaster recovery, data replication, and management of the Singha Durbar Network. These services help government agencies maintain secure, reliable, and uninterrupted digital operations while improving the efficiency of public service delivery.

In addition to its technical services, the IDMC website functions as an information portal where visitors can access tender notices, procurement announcements, official publications, downloadable resources, media updates, and various online services. By making this information publicly available, the center promotes transparency, improves communication with stakeholders, and supports the effective implementation of secure digital services throughout Nepal's public sector. Overall, IDMC plays a vital role in strengthening the nation's digital infrastructure and accelerating the adoption of e-Governance.

As part of the Cloud Computing course in the Bachelor of Computer Application (BCA) program, our class conducted an educational field visit to the Integrated Data Management Center on 24 June 2026. The visit aimed to bridge the gap between theoretical concepts learned in the classroom and their practical implementation in a real-world environment. It provided us with first-hand exposure to technologies such as virtualization, resource pooling, cloud infrastructure, and data center management. More importantly, it helped us understand how a national-level government data center is designed, secured, and managed to support the digital services and e-Governance systems used throughout Nepal.

CHAPTER 2: OBJECTIVES

The visit to the Integrated Data Management Center (formerly GIDC) was conducted with the following objectives:

- To gain practical insight into the infrastructure, cloud computing environment, and digital services operated by the Integrated Data Management Center, and to understand how they support government institutions and Nepal's e-Governance initiatives.
- To study the security, backup, and disaster recovery mechanisms implemented by the center to ensure the protection, reliability, and continuous availability of critical government data and digital services.

CHAPTER 3: FIELD OBSERVATION

During the visit, our attention was directed at the physical infrastructure, cloud architecture, service catalogue, security mechanisms, and disaster recovery arrangements maintained at the Integrated Data Management Center. What follows is organized by the specific area of the facility that was shown to us.

3.1 Infrastructure Used

The **Integrated Data Management Center (IDMC)**, formerly known as the **Government Integrated Data Center (GIDC)**, is Nepal's primary government data center responsible for hosting and managing digital services for ministries, departments, constitutional bodies, and other public sector organizations. Located within the Singha Durbar complex in Kathmandu, the facility provides a secure, reliable, and highly available computing environment that supports the Government of Nepal's e-Governance initiatives. During our visit, we observed the major components that work together to ensure uninterrupted operation of government digital services.

Data Center Building and Physical Security

The data center is situated inside a highly secured government compound with strict physical security measures. Access to sensitive areas, including the server rooms, is limited to authorized personnel only. Multiple layers of access control are implemented to prevent unauthorized entry, and visitors are required to complete security verification before entering restricted areas. Inside the server rooms, the equipment is neatly organized in dedicated server racks with structured cable management systems, while environmental monitoring devices continuously track temperature, humidity, and other operating conditions to ensure the safe functioning of critical infrastructure.

Server Infrastructure

The server infrastructure consists of enterprise-grade rack-mounted servers designed to support large-scale government applications. These servers host a wide range of services, including government websites, databases, web applications, email systems, and various digital platforms used by public organizations. One of the key technologies employed is **virtualization**, which allows a single physical server to be divided into multiple

independent Virtual Machines (VMs). This approach enables efficient utilization of hardware resources while providing isolated and secure environments for different government agencies.

Storage Infrastructure

To securely manage the large volume of government data, IDMC utilizes centralized enterprise storage systems based on **Storage Area Network (SAN)** technology. The storage infrastructure supports databases, document repositories, online government services, backup operations, and disaster recovery mechanisms. Since multiple servers can simultaneously access the centralized storage, data management becomes more efficient, scalable, and reliable.

Network Infrastructure

The center operates on a high-speed backbone network that interconnects ministries, departments, and other government institutions throughout Nepal. The network is supported by enterprise routers, Layer-3 switches, firewalls, and network monitoring systems that ensure secure and reliable communication between government organizations. During the visit, we also learned about the **Singha Durbar Network (SDN)**, a centralized network managed by IDMC that enables secure data exchange and communication among government offices located within the Singha Durbar premises.

Power Infrastructure

Since uninterrupted operation is essential for government services, the data center employs a highly reliable power infrastructure. Electricity is supplied through commercial power lines and is supported by multiple backup systems, including **Uninterruptible Power Supply (UPS)** units, battery banks, and standby diesel generators. This layered approach ensures that servers continue operating without interruption even during power failures, minimizing downtime and protecting critical government services.

Cooling and Environmental Control

Server equipment generates a considerable amount of heat during operation. To maintain an optimal operating environment, the data center uses dedicated **Heating, Ventilation,**

and Air Conditioning (HVAC) systems that regulate temperature and humidity within the server rooms. Environmental monitoring systems continuously measure these conditions and immediately alert administrators if any abnormal changes occur. Proper cooling not only prevents equipment failure but also improves system reliability and extends the lifespan of the hardware.

Backup and Disaster Recovery Infrastructure

Protecting government data is one of the center's highest priorities. IDMC maintains centralized backup, replication, and disaster recovery facilities to ensure business continuity in the event of hardware failure, cyberattacks, natural disasters, or other unexpected incidents. Important government data is backed up regularly, allowing systems to be restored quickly whenever necessary. These mechanisms significantly reduce the risk of permanent data loss and help maintain uninterrupted public services.

Cloud Computing Infrastructure

One of the most important aspects observed during the visit was IDMC's **Government Cloud Infrastructure**, which operates on the **Infrastructure as a Service (IaaS)** model. Using virtualization technology, computing resources such as processing power, memory, storage, and networking are dynamically allocated to government organizations based on their operational needs. This centralized cloud platform improves scalability, optimizes resource utilization, reduces infrastructure costs, and simplifies the management of government IT services while maintaining high levels of security and availability.

Monitoring and Operations Center

The Monitoring and Operations Center continuously supervises the health and performance of servers, storage systems, networking equipment, power infrastructure, and environmental conditions throughout the facility. Advanced monitoring tools allow technical personnel to identify faults, analyze system performance, and respond quickly to operational issues before they affect government services. This proactive monitoring approach helps maintain the high availability and reliability required for mission-critical government applications.

3.2 Services Provided

The **Integrated Data Management Center (IDMC)** provides a wide range of information technology services that support the digital operations of government ministries, departments, constitutional bodies, and other public sector organizations. During our visit, we learned that the center primarily operates as a **private government cloud**, where computing resources and digital services are made available exclusively to government institutions. These services play a vital role in ensuring secure, reliable, and efficient delivery of e-Governance services across Nepal, the services offered are as follows:

Domain Registration Service

One of the fundamental services offered by IDMC is **Domain Registration** for government organizations. The center manages the registration and administration of official government domain names, particularly those under the **.gov.np** domain. This service ensures that every government institution has a secure and authentic online identity that can be easily recognized by citizens. Before a domain is approved, the requesting organization undergoes proper verification to maintain the credibility and integrity of government websites. In addition to registration, IDMC also provides Domain Name System (DNS) configuration and technical support, enabling organizations to connect their websites with hosting services and other digital platforms.

Internet Service

IDMC provides reliable **Internet Services** to government agencies, enabling them to access cloud infrastructure, online applications, and digital communication platforms. The service is supported by a high-speed network backbone and is continuously monitored to ensure stable connectivity with minimal downtime. Reliable internet access is essential for delivering online public services, facilitating communication between government organizations, and supporting the day-to-day operation of various e-Governance systems. Through this service, IDMC helps maintain uninterrupted digital operations across the public sector.

Virtual Machine (VM) / Virtual Private Server (VPS)

To reduce the need for organizations to maintain their own physical servers, IDMC offers **Virtual Machine (VM)** and **Virtual Private Server (VPS)** services.. Government organizations can use these virtual environments to host websites, databases, enterprise applications, and other digital services in a secure and scalable manner. This approach improves resource utilization, reduces infrastructure costs, simplifies system management, and provides flexibility to allocate resources according to organizational requirements.

Server Colocation Service

The **Server Colocation Service** allows government organizations to place their own physical servers within the professionally managed infrastructure of the Integrated Data Management Center. Instead of building and maintaining separate server rooms, organizations can benefit from IDMC's secure facilities, including rack space, redundant power supply, high-speed network connectivity, cooling systems, and physical security controls. Although the hardware remains the property of the respective organizations, the hosting environment is maintained by IDMC, ensuring improved reliability, better security, and reduced operational overhead.

Backup and Replication Service

To protect critical government information, IDMC provides comprehensive **Backup and Replication Services**. Important data is backed up regularly to prevent loss resulting from hardware failures, accidental deletion, cyberattacks, or natural disasters. In addition to maintaining scheduled backups, the center also replicates data to disaster recovery facilities, allowing government organizations to restore their systems quickly in the event of a major failure. These services play a crucial role in ensuring business continuity, minimizing downtime, and maintaining the availability of essential public services.

Singha Durbar Network (SDN)

The **Singha Durbar Network (SDN)** is one of the major network infrastructures managed by IDMC. It provides secure and centralized communication between ministries, departments, and government agencies located within the Singha Durbar complex. The network enables efficient sharing of information, access to common government resources,

and secure communication among different organizations. By maintaining a dedicated government network, IDMC improves coordination between public institutions while strengthening the overall security and efficiency of Nepal's e-Governance infrastructure.

3.3 Security Measures

Security is one of the most critical aspects of the **Integrated Data Management Center (IDMC)**, as it hosts and manages sensitive government information and digital services. During our visit, we observed that the center follows a **multi-layered security approach**, combining strict physical security measures with advanced network security mechanisms to protect its infrastructure from both physical and cyber threats.

Physical Security

The data center is located within the highly secured Singha Durbar government premises, where access is carefully monitored and controlled. Entry into the facility is restricted to authorized personnel, while access to critical areas such as the server rooms requires multiple levels of identity verification. During the visit, we observed that several security checkpoints must be cleared before entering the server area. Biometric authentication and electronic access control systems are used to ensure that only authorized individuals can enter sensitive operational zones. Every access attempt is recorded and monitored through a centralized Identity and Access Management (IAM) system, providing accountability and preventing unauthorized access to critical government infrastructure.

The importance of these physical security measures was demonstrated during the September 2025 protests near the Singha Durbar complex. Although nearby government buildings were affected by fire, the Integrated Data Management Center remained secure due to its strong physical protection and the continuous efforts of technical personnel who monitored the facility throughout the incident. As a result, essential government digital services continued to operate without significant disruption.

Network Security

In addition to physical protection, IDMC employs several advanced network security technologies to safeguard its digital infrastructure from cyber threats. Enterprise-grade **Next-Generation Firewalls (NGFWs)** inspect incoming and outgoing network traffic,

block unauthorized access, and enforce security policies before traffic reaches internal systems. These firewalls provide comprehensive protection by analyzing traffic across multiple layers of the network.

To defend against **Distributed Denial-of-Service (DDoS)** attacks, the center utilizes dedicated **traffic scrubbing systems** that detect malicious traffic and filter it before it reaches production servers. These mechanisms help maintain the availability of government websites and online services even during large-scale cyberattacks.

During the visit, officials also explained that the data center continuously monitors network traffic, server activity, and security events using centralized monitoring tools. This enables technical teams to quickly detect suspicious activities, respond to potential security incidents, and minimize risks before they affect government services.

Cybersecurity Challenges

Although IDMC has implemented robust security measures, cybersecurity remains an ongoing challenge due to the increasing number and sophistication of cyber threats. Officials shared that government digital infrastructure has experienced cyberattacks in recent years, highlighting the importance of continuously strengthening security mechanisms. In response, government agencies have been encouraged to adopt stronger cybersecurity practices such as **multi-factor authentication (MFA)**, regular software updates, vulnerability assessments, network segmentation, and continuous security monitoring.

The visit emphasized that cybersecurity is not solely dependent on the infrastructure managed by IDMC. Individual government organizations also play an important role by maintaining secure systems, regularly backing up their data, applying security updates, and following established cybersecurity policies. Effective security therefore requires close coordination between the data center and the agencies that use its services.

3.4 Disaster Recovery Plan

A **Disaster Recovery (DR) Plan** is a critical component of any modern data center, ensuring that essential services can continue operating even in the event of natural disasters, cyberattacks, hardware failures, or other unexpected incidents. During our visit to the

Integrated Data Management Center (IDMC), we learned that disaster recovery is one of the organization's highest priorities because it hosts many mission-critical government systems that must remain available at all times.

To strengthen business continuity, IDMC has established a dedicated **Disaster Recovery (DR) Center** in **Hetauda**, geographically separated from the primary data center located at Singha Durbar, Kathmandu. The disaster recovery site was developed as part of the second phase of a Korean Official Development Assistance (ODA) project supported by the **Korea International Cooperation Agency (KOICA)**. Although the project experienced delays following the 2015 earthquake, the Hetauda facility was officially inaugurated in 2019, and additional improvements were completed in 2021 to further enhance its disaster recovery capabilities.

The primary objective of maintaining a geographically separate disaster recovery site is to ensure that government digital services remain operational even if the main data center becomes unavailable. Locating the backup facility in a different seismic region minimizes the possibility of both sites being affected by the same natural disaster, such as a major earthquake. During the visit, officials also mentioned plans to establish additional disaster recovery facilities in other regions of Nepal to further improve service resilience and reduce dependency on a single backup location.

A key technology supporting this disaster recovery strategy is **asynchronous data replication**. Under this approach, data generated at the primary data center is first written to the local storage system and is then replicated to the Hetauda disaster recovery site after a short interval. Compared to synchronous replication, asynchronous replication introduces very little performance overhead because applications do not need to wait for confirmation from the remote site before processing requests. Although this method may result in a small amount of data loss if a failure occurs before replication is completed, the potential loss is minimized by maintaining short replication intervals. This acceptable amount of potential data loss is measured using the **Recovery Point Objective (RPO)**.

The disaster recovery infrastructure is complemented by centralized backup systems that allow government applications, databases, and digital services to be restored quickly whenever failures occur. Together, data replication, regular backups, and geographically

separated recovery facilities provide multiple layers of protection against system failures, ensuring business continuity and minimizing service downtime.

The effectiveness of this disaster recovery strategy was demonstrated during the **September 2025 protests** near the Singha Durbar complex. Despite fires occurring within the surrounding government premises, both the primary data center in Kathmandu and the disaster recovery facility in Hetauda remained fully operational. Technical personnel continuously monitored the infrastructure throughout the incident, enabling essential government services including the **Nagarik App** and the **National ID System** to remain available without significant interruption. This real-world event highlighted the importance of maintaining redundant infrastructure and implementing a well-planned disaster recovery strategy.

3.5 Backup and Recovery

The **Backup and Recovery** system implemented at the **Integrated Data Management Center (IDMC)** is designed to protect critical government data and ensure that digital services can be restored quickly in the event of system failures, cyberattacks, accidental data loss, or natural disasters. During our field visit, we learned that data protection is treated as a continuous operational process rather than an occasional maintenance activity. This approach helps maintain the availability, integrity, and reliability of government information systems.

To safeguard important government data, IDMC performs **scheduled backups** at regular intervals using enterprise-level storage infrastructure. The center utilizes **Storage Area Network (SAN)** technology to create automated snapshots and full backups of government databases, applications, and digital records. These backups provide multiple restore points, enabling administrators to recover systems efficiently whenever data is corrupted, accidentally deleted, or affected by hardware failures.

The backup infrastructure is designed using a **tiered storage approach** to balance performance and cost. Frequently accessed and active data is stored on high-speed **Solid-State Drives (SSDs)** to provide faster processing and improved application performance. In contrast, backup data and long-term archives are stored on higher-capacity **Hard Disk Drives (HDDs)**, which offer a more economical solution for retaining large volumes of

government data over extended periods. This combination allows the center to maintain both high system performance and cost-effective data storage.

In addition to local backups, IDMC strengthens its recovery capability by replicating critical government data to the **Disaster Recovery (DR) Center in Hetauda**. This off-site replication ensures that a secondary copy of important information remains available even if the primary data center becomes unavailable due to a major disaster. By combining local SAN-based backups with geographically separated disaster recovery infrastructure, the center provides multiple layers of protection against data loss and service disruption.

During the visit, officials also explained that backup responsibility is **shared between IDMC and the individual government organizations** that host their systems within the data center. While IDMC provides the centralized backup infrastructure and disaster recovery facilities, each organization is responsible for ensuring that its applications and critical datasets are properly configured for backup according to its operational requirements. As a result, the level of protection may vary depending on how individual agencies manage their own backup policies and recovery procedures.

Recovery operations are supported by continuous monitoring and periodic verification of backup systems to ensure that stored data remains complete, consistent, and recoverable. These routine checks help identify potential issues before an actual emergency occurs, allowing technical teams to maintain confidence in the recovery process and minimize downtime during system failures.

3.6 Future Plans

During our visit to the **Integrated Data Management Center (IDMC)**, officials discussed several future initiatives aimed at strengthening Nepal's government cloud infrastructure and supporting the country's ongoing digital transformation. These plans focus on expanding infrastructure capacity, improving cybersecurity, enhancing disaster resilience, strengthening data governance, and adopting emerging technologies to meet the increasing demand for secure and reliable government digital services.

One of the center's primary goals is the **expansion of geographically distributed data centers** across Nepal. While the existing Disaster Recovery Center in Hetauda already

provides redundancy for the primary data center in Kathmandu, officials indicated that establishing additional facilities in different regions would further improve disaster preparedness, reduce dependence on a single backup location, and ensure continuous availability of government services during natural disasters or major infrastructure failures. This approach aligns with international best practices for business continuity and resilient cloud infrastructure.

Another major area of focus is **strengthening cybersecurity**. As government digital services continue to expand, protecting critical infrastructure against cyber threats has become increasingly important. The center plans to enhance its security posture through regular security audits, vulnerability assessments, continuous monitoring, stronger access control mechanisms, improved firewall protection, and well-defined incident response procedures. These measures are intended to safeguard sensitive government information while ensuring the confidentiality, integrity, and availability of public digital services.

The officials also highlighted the importance of **data governance and data sovereignty**. Future initiatives include establishing comprehensive policies for data classification, storage management, access control, retention, and privacy protection. Strengthening governance frameworks will help ensure that government data remains secure, properly managed, and stored in accordance with national regulations while supporting trusted digital public services. These efforts are consistent with Nepal's **Digital Nepal Framework** and the recently published **Data Center and Cloud Service Operation and Management Directive, 2081**, which provide strategic guidance for the development and operation of government cloud services.

Further improvements are planned for **backup and disaster recovery capabilities**. Officials explained that the center intends to strengthen replication technologies, expand disaster recovery infrastructure, and continuously improve recovery procedures to reduce service downtime and minimize the risk of data loss. Along with geographically separated recovery sites, these improvements will ensure that essential government services remain available even during large-scale emergencies.

The center also plans to invest in **power and network redundancy** by upgrading backup power systems, improving cooling infrastructure, and maintaining multiple network connectivity options. Reliable power supply and uninterrupted network connectivity are

fundamental requirements for maintaining high availability within a government cloud environment, and these upgrades will further improve the operational stability of the data center.

Recognizing that technology alone is not sufficient, IDMC places significant emphasis on **developing skilled technical manpower**. Officials explained that continuous training in cloud computing, virtualization, cybersecurity, network administration, disaster recovery, and infrastructure management will remain a priority. Strengthening the knowledge and technical expertise of staff will improve operational efficiency while reducing dependence on external specialists.

Another important initiative is the development of **strong government cloud governance frameworks**. The center aims to establish standardized guidelines covering cloud adoption, service delivery, security compliance, resource allocation, and operational management. Such governance frameworks will encourage government agencies to adopt cloud technologies in a consistent, secure, and well-managed manner while ensuring compliance with national ICT policies and regulations.

Officials also emphasized the importance of **public-private partnerships** in accelerating digital transformation. Collaborating with technology companies, academic institutions, and industry experts will enable the government to benefit from modern technologies, specialized expertise, and innovative solutions while maintaining strict security standards and government oversight. Such partnerships are expected to support the modernization of Nepal's digital infrastructure and improve the quality of public digital services.

Looking ahead, the center plans to explore the adoption of **Artificial Intelligence (AI), automation, and intelligent monitoring technologies**. These emerging technologies have the potential to improve infrastructure monitoring, automate routine administrative tasks, strengthen cybersecurity through intelligent threat detection, optimize resource allocation, and enhance the efficiency of government service delivery. As Nepal continues its digital transformation journey, these technologies are expected to play an increasingly important role in supporting secure, transparent, and citizen-centric public services. This vision aligns closely with Nepal's broader digital transformation strategy and recent investments in digital infrastructure and governance.

CHAPTER 4: LEARNINGS

The field visit to the **Integrated Data Management Center (IDMC)** provided an excellent opportunity to connect the theoretical concepts studied in the Cloud Computing course with their practical implementation in a real-world government data center. Observing the infrastructure, cloud services, and operational procedures firsthand helped us better understand how modern technologies are used to support Nepal's e-Governance initiatives. The key learning outcomes from the visit are summarized below:

- **Practical Understanding of Data Center Operations:** We gained first-hand knowledge of how enterprise servers, storage systems, networking equipment, and cloud infrastructure work together to provide secure, reliable, and highly available digital services for multiple government organizations.
- **Understanding of Virtualization and Cloud Computing:** The visit enhanced our understanding of virtualization technologies and the Infrastructure as a Service (IaaS) model. We observed how physical servers are divided into multiple Virtual Machines (VMs), allowing computing resources to be shared efficiently while maintaining security, scalability, and performance.
- **Knowledge of Enterprise Storage Systems:** We learned how centralized Storage Area Network (SAN) technology enables efficient storage management, supports government applications, and facilitates backup and disaster recovery operations.
- **Importance of Physical and Cybersecurity:** The visit emphasized the importance of implementing multiple layers of security to protect sensitive government information. Physical access control, biometric authentication, enterprise firewalls, network monitoring systems, and Identity and Access Management (IAM) mechanisms collectively help safeguard critical digital infrastructure against unauthorized access and cyber threats.
- **Understanding of Backup and Disaster Recovery:** We developed a better understanding of how scheduled backups, data replication, and geographically separated disaster recovery facilities help maintain business continuity and minimize service disruption during hardware failures, cyber incidents, or natural disasters.
- **Awareness of Infrastructure Reliability:** We observed the importance of redundant power supplies, UPS systems, diesel generators, cooling infrastructure,

and continuous environmental monitoring in ensuring uninterrupted operation of mission-critical government services.

- **Understanding the Role of IDMC in Nepal's Digital Transformation:** The visit demonstrated how centralized cloud infrastructure, secure hosting services, government networking, domain management, and disaster recovery facilities support the implementation of e-Governance and improve public service delivery throughout Nepal.
- **Importance of Skilled Technical Professionals:** Managing a modern government data center requires expertise in cloud computing, virtualization, networking, cybersecurity, storage management, and system administration. The visit highlighted the crucial role played by technical personnel in maintaining the reliability and security of national digital infrastructure.
- **Appreciation of Modern Data Center Management:** The visit provided valuable insight into how monitoring systems, preventive maintenance, security policies, and standardized operational procedures work together to ensure the continuous availability and efficiency of government digital services.
- **Application of Classroom Knowledge:** Most importantly, the field visit allowed us to relate theoretical concepts such as cloud computing, virtualization, resource pooling, disaster recovery, backup strategies, and network security to their practical implementation in a large-scale government cloud environment. This significantly strengthened our understanding of the Cloud Computing course.

CHAPTER 5: CONCLUSION

The field visit to the **Integrated Data Management Center (IDMC)** was an enriching and valuable learning experience that bridged the gap between classroom theory and real-world practice. It provided us with practical exposure to the technologies, infrastructure, and operational procedures used to manage Nepal's national government cloud infrastructure and support a wide range of e-Governance services.

Throughout the visit, we observed how cloud computing technologies, virtualization, enterprise storage systems, centralized networking, and Infrastructure as a Service (IaaS) are integrated to deliver secure, reliable, and scalable digital services to government ministries, departments, and public agencies. We also gained a deeper appreciation for the importance of physical security, cybersecurity, backup strategies, disaster recovery planning, and continuous monitoring in ensuring the availability and protection of critical government information.

The visit further demonstrated that operating a modern government data center involves much more than maintaining servers. It requires careful planning, skilled technical personnel, robust infrastructure, effective resource management, and well-defined security and disaster recovery strategies. These elements work together to ensure uninterrupted delivery of digital public services and support Nepal's ongoing digital transformation.

Overall, the field visit significantly enhanced our understanding of cloud computing and data center technologies by allowing us to observe their practical implementation in a real operational environment. The knowledge and experience gained from this visit will serve as a strong foundation for our future academic studies and professional careers in cloud computing, networking, cybersecurity, system administration, and information technology.

REFERENCES

- Baral, U. K., & Gurung, D. (n.d.). *Data Center Development in Nepal's Digital Infrastructure: Benefits, Challenges and Strategic Priorities*. Retrieved from https://www.researchgate.net/publication/405023334_Data_Center_Development_in_Nepal's_Digital_Infrastructure_Benefits_Challenges_and_Strategic_Priorities
- Scribd. (n.d.). *GIDC Nepal*. Retrieved from <https://www.scribd.com/presentation/986295481/GIDC-Nepal>
- Suchanaa. (n.d.). *Integrated Data Management Center*. Retrieved from <https://suchanaa.com/directory/integrated-data-management-center/>
- Integrated Data Management Center. (2025). *Data Center and Cloud Service Operation and Management Directive, 2081*. Retrieved from <https://suchanaa.com/directory/integrated-data-management-center/>
- Department of Information Technology, Government of Nepal. (n.d.). *Digital Government Services and ICT Initiatives*. Retrieved from <https://doit.gov.np>

APPENDIXES



Appendix A: Singha Durbar, Kathmandu – Outside Administrative complex housing the GIDC/IDMC facility.



Appendix B: Inside GIDC/IDMC facility.