SET 6

Group 'A' (Long questions)

Attempt any TWO questions 2x10=20

1. What is the Present Global Trends of Growth in E-Governance?
2. Explain E-Government Security Architecture with proper diagram.
3. Define data mining and data warehouse. Explain their implementation and application in e governance.

Group 'B' (Short questions)

Attempt all the questions (8x5=40)

1. What is Computing Infrastructure? Explain.
2. Define Human Resource Management Software. Write about its benefit.
3. Explain about Cyber Law in Nepal.
4. How can we use E governance model to achieve good governance? Discuss
5. What are the issues related to E governance application? Why do we need to consider these issues?
6. What are the various Security Approaches for E-Government?
7. Write short note on Ekal Seva Kendra.
8. Define Comparative Analysis Model with proper application and diagram.

Answer of Set-6

1. **What is the Present Global Trends of Growth in E-Governance?**

Ans: The Present Global Trends of Growth in E-Governance are described below:

Rapid adoption of digital technologies:

- Governments are increasingly leveraging technologies like Cloud Computing, Artificial Intelligence (AI), and Internet of Things (IoT) to improve public service delivery.
- The COVID-19 pandemic has accelerated this digital transformation in the public sector.

Focus on citizen-centric services:

- Governments are designing digital services and platforms that are tailored to the needs and preferences of citizens.
- This includes user-friendly interfaces, multi-channel access, and personalized services.

Increased transparency and accountability:

- E-governance initiatives are aimed at enhancing transparency and accountability in government operations.
- This includes the use of open data platforms, online public consultations, and real-time monitoring of government performance.

Integration and collaboration across government agencies:

- Governments are integrating various agencies and departments through e-governance platforms.
- This enables seamless information sharing and service delivery across different domains.

Shift towards mobile-first approach:

- The widespread adoption of smartphones has led to a focus on developing mobile-friendly government applications and services.
- This allows citizens to access services and information anytime, anywhere.

Exploration of emerging technologies:

- Governments are exploring the use of emerging technologies like block chain, RPA, and AR/VR to enhance the efficiency, security, and user experience of e-governance services.

Global collaboration and knowledge sharing:

- There is an increasing trend of international collaboration and knowledge sharing among governments.
- This helps to accelerate the global adoption and advancement of e-governance initiatives.

Cybersecurity and Data Privacy:

- Governments are making sure that information they have is safe from bad people on the internet.
- They're also making rules to keep people's personal information private when they use government services online.

AI and Automation:

- Governments are using smart computer programs to do jobs that people used to do, like answering questions or making decisions.
- This helps make things faster and cheaper for the government.

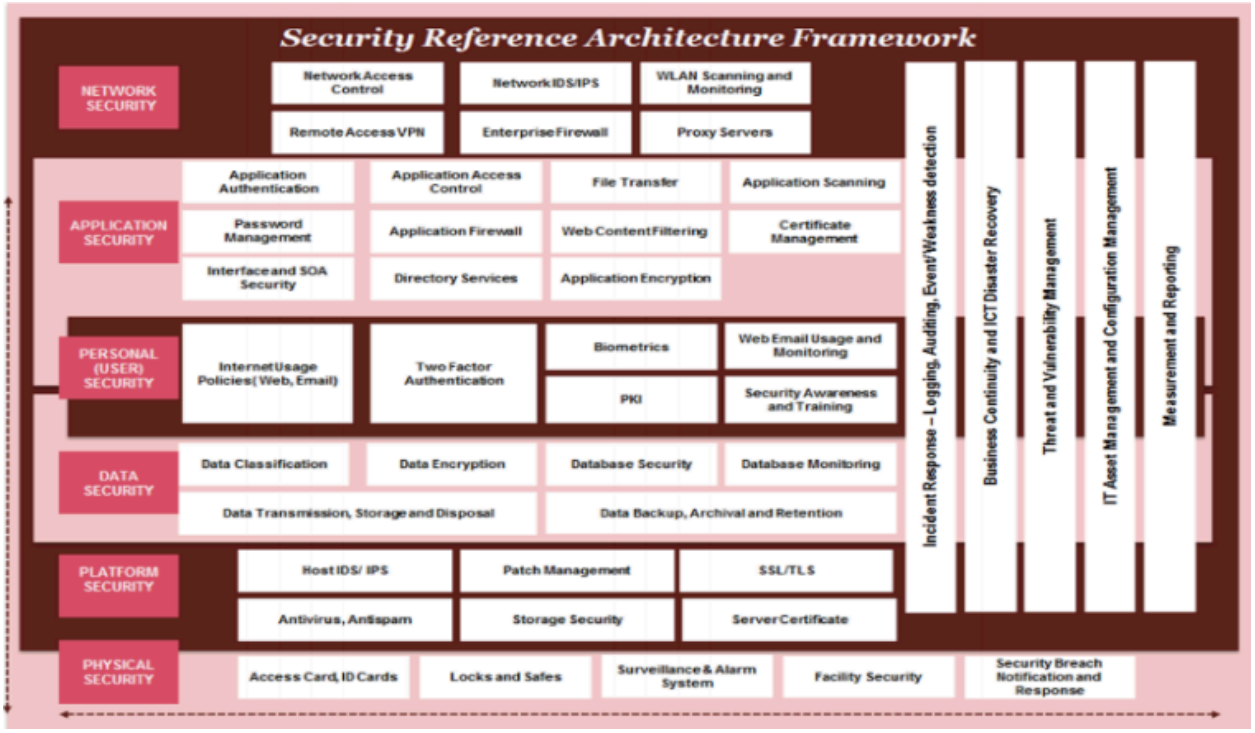
Blockchain for Governance:

- Governments are using a special kind of technology called blockchain to keep track of important things like who owns what or who voted in an election.
- This makes it really hard for people to cheat or lie about these things because it's all recorded in a special way.

In conclusion, e-governance trends focus on using technology to make government services more accessible, transparent, and efficient. By embracing digital transformation, promoting citizen engagement, and ensuring cybersecurity, governments aim to meet the evolving needs of citizens in the digital age.

2. **Explain E-Government Security Architecture with proper diagram.**

Ans:



E-Government Security Architecture refers to the comprehensive framework of policies, procedures, technologies, and practices designed to secure electronic government systems, data, and infrastructure from various cyber threats and vulnerabilities. It encompasses multiple layers of security measures, including network security, application security, data security, personnel/user security, platform/host security, and physical security. The primary goal of E-Government Security Architecture is to safeguard government digital assets, sensitive information, and online services against unauthorized access, data breaches, cyber-attacks, and other security risks. It involves the implementation of robust security controls, such as authentication mechanisms, encryption, access controls, intrusion detection systems, firewalls, and security monitoring tools.

1. Network Security: This layer focuses on safeguarding the network infrastructure through robust authentication mechanisms, firewall protection, and network intrusion detection systems. These measures are crucial in preventing unauthorized access and detecting and mitigating potential threats.

2.Application Security: Utilizing a combination of software, hardware, and procedural methods, application security shields government applications from

external threats. This includes secure coding practices, encryption, access controls, and regular security assessments to identify and address vulnerabilities.

3.Personnel/User Security: Various authentication mechanisms, such as two-factor authentication and biometrics, are employed to verify user identities, ensuring that only authorized personnel can access sensitive government systems and data.

4.Data Security: Data security mechanisms are implemented to protect data from corruption and unauthorized access, preserving data privacy through encryption, access controls, and data integrity checks.

5.Platform/Host Security: Platform security involves implementing robust security measures on servers, workstations, and operating systems to prevent unauthorized access and ensure the security and integrity of government systems.

6.Physical Security: Physical security measures restrict physical access to government facilities and equipment, preventing unauthorized personnel from compromising critical infrastructure.

Cross Pillar

1.2Incident Response: Establishing procedures to promptly address and manage security breaches or attacks is essential. Incident response plans outline the steps to mitigate the impact of security incidents and restore normal operations swiftly.

2.Business Continuity and ICT Disaster Recovery: These pillars ensure that essential government functions and ICT operations can continue during and after a disaster. Comprehensive continuity and recovery plans minimize downtime and ensure the resilience of government services.

3.Threat and Vulnerability Management: Identifying and mitigating risks in the ICT environment is critical. Threat and vulnerability management processes continuously assess the security posture, identify potential vulnerabilities, and implement controls to mitigate risks effectively.

4.ICT Asset Management: Managing ICT assets throughout their lifecycle is vital for ensuring their security and availability. Proper asset management practices encompass procurement, deployment, maintenance, and disposal, ensuring that assets are adequately protected and accounted for.

5.Measurement and Reporting: Providing regular assessments of the health and security status of ICT appliances and systems is crucial. Measurement and

reporting mechanisms offer insights into the effectiveness of security measures and enable continuous improvement.

3. **Define data mining and data warehouse. Explain their implementation and application in e-governance.**

Ans:

Data Mining: Data mining is the process of extracting valuable insights, patterns, and knowledge from large datasets. It involves using various statistical, mathematical, and machine learning techniques to analyze data and extract valuable knowledge.

Data Warehousing: A data warehouse is a central repository that stores and consolidates historical data extracted from various sources within an organization, with the goal of providing a unified and comprehensive view of the data and designed for analysis and is optimized for reporting and decision support.

Applications:

- **Agriculture:**
  Data Warehousing: Build a central repository for agricultural census, crop, fertilizer, livestock, and land use data.
  Data Mining: Analyze the data to uncover patterns, trends, and insights to support better policymaking and resource allocation in the agricultural sector.

- **Rural Development:**
  Data Warehousing: Consolidate data on poverty, drinking water, and rural development program implementation.
  Data Mining: Apply techniques like clustering and predictive modeling to identify underserved areas, optimize resource distribution, and monitor program effectiveness.

- **Health:**

Data Warehousing: Integrate community needs, immunization, and national health program data into a centralized data warehouse.
Data Mining: Leverage the data to detect disease outbreaks, analyze healthcare utilization patterns, and inform targeted interventions.

- **Planning:**
  Data Warehousing: Create a comprehensive data warehouse to store and manage country-wide survey data.
  Data Mining: Use the data to identify regional disparities, evaluate the impact of development plans, and inform future policy decisions.

- **Education:**
  Data Warehousing: Consolidate trade, world price, and import/export data for analysis.
  Data Mining: Apply forecasting techniques to improve the accuracy of trade estimates and support trade policy formulation.

- **Commerce and Trade:**
  Data Warehousing: Build a centralized repository for trade, world price, and import/export data.
  Data Mining: Analyze the data to identify trade patterns, monitor market trends, and enhance the effectiveness of trade policies.

4. **What is Computing Infrastructure? Explain.**

Ans:

Computing infrastructure refers to the entire foundation of resources and technology that supports the computing operation, data storage and information processing within an organization. Computing infrastructure for e-governance includes the hardware (servers, storage, network devices), software (operating systems, applications, security tools), and connectivity (WAN, LAN, internet) that enable the delivery of digital government services and information.

Components:

Hardware: Physical components like servers, storage devices, and networking equipment. These house the data, applications, and functionalities that power e-government services.

Software: Operating systems, database management systems, and e-government application software. These programs manage hardware resources, store and organize data, and deliver specific services to users.

Networks: Communication channels that connect various components within the infrastructure and allow users to access e-government services online. This includes the internet, local area networks (LANs), and wide area networks (WANs).

Data Centers: Secure facilities that house the physical hardware components like servers and storage. They provide a controlled environment with power, cooling, and security measures to ensure the smooth operation of e-government systems.

Cloud Computing: Cloud computing means using the internet to store and access data and programs instead of keeping them on individual computers, which makes it easier for the government to manage and share information online.

Security Measures: Security measures are like locks and alarms for government data, they keep it safe from bad guys who might try to steal or mess with it, making sure only the right people can access it.

5. Define Human Resource Management Software. Write about its benefit.

Ans:

Human Resource Management (HRM) software refers to the digital systems and tools used to manage and automate various HR-related functions and processes within an organization. In the context of e-governance, HRM software can play a significant role in improving the efficiency and effectiveness of government human resource management and utilized to manage government employees' information, recruitment processes, payroll, performance evaluation, training, and other HR functions.

Benefits:

- **Streamlined HR Processes:** Automates and digitizes HR functions like onboarding, payroll, and attendance tracking.
- **Improved Employee Data Management:** Provides a centralized database for employee information and ensures compliance.
- **Enhanced Workforce Planning and Talent Management:** Supports workforce analysis, skills gap identification, and talent management activities.
- **Increased Employee Engagement and Communication:** Offers self-service portals and collaboration tools to engage employees.
- **Compliance and Regulatory Adherence:** Helps government agencies maintain compliance with labor laws and regulations.
- **Data-Driven Decision-Making:** Enables data-informed decisions on workforce planning and employee development.
- **Data-Driven Decision-Making:** Enables data-informed decisions on workforce planning and employee development.

6. **Explain about Cyber Law in Nepal.**

Ans:

Cyber law is an important and evolving domain that deals with the legal issues arising from the use of digital technologies, the internet, and electronic communications. It typically covers areas such as data protection, privacy, cybercrime, e-commerce, and intellectual property rights in the digital space.

In Nepal, cyber law is primarily governed by the Electronic Transactions Act, 2063 (2008), which legalizes electronic transactions and establishes rules for data protection. This act recognizes the validity of electronic documents, signatures, and contracts, facilitating online commerce and transactions. Additionally, it mandates organizations and individuals to implement measures to safeguard electronic data and information systems from unauthorized access or alteration, ensuring data security and privacy.

Furthermore, Nepal enacted the Cyber Crime and Cyber Security Act, 2074 (2017), to address cyber offenses and enhance cybersecurity measures. This legislation criminalizes various cybercrimes, including hacking, cyber fraud, and dissemination of malicious software. It also establishes the Cyber Bureau within the Nepal Police to investigate and prosecute cybercrimes effectively. Overall, these laws aim to promote the safe and secure use of technology, deter cyber threats, and protect the rights and interests of individuals and organizations in cyberspace.

7. **How can we use E governance model to achieve good governance? Discuss.**

Utilizing an e-governance model can significantly contribute to achieving good governance by enhancing transparency, efficiency, accountability, and citizen engagement. Here's a discussion on how e-governance can facilitate good governance:

I. Transparency: E-governance platforms can provide citizens with easy access to information about government policies, programs, and activities. Through online portals and digital databases, citizens can access public records, budgets, procurement information, and decision-making processes. Transparency builds trust between the government and its citizens, fostering accountability and reducing corruption.

II. Efficiency: E-governance streamlines bureaucratic processes and reduces administrative burdens by digitizing workflows, automating tasks, and enabling online transactions. This efficiency leads to cost savings, faster service delivery, and improved resource allocation. For example, online tax filing systems, digital permit applications, and electronic document management systems streamline processes, reducing delays and paperwork.

III. Accountability: E-governance models incorporate mechanisms for tracking government actions, expenditures, and performance. Online reporting tools, dashboards, and performance metrics enable citizens to monitor government activities and hold public officials accountable for their decisions. Additionally, digital audit trails and transparency in decision-making processes contribute to accountability and discourage malfeasance.

IV. Citizen Engagement: E-governance platforms facilitate direct communication between citizens and government agencies, enabling feedback, participation, and collaboration. Online forums, social media channels, and mobile applications provide avenues for citizens to voice concerns, submit suggestions, and participate in public consultations. Engaging citizens in policymaking processes promotes inclusivity, responsiveness, and legitimacy in governance.

V. Access to Services: E-governance enhances access to government services by providing convenient online channels for citizens to interact with government agencies. Through e-services portals, citizens can apply for permits, licenses, benefits, and other services from the comfort of their homes or offices, reducing the need for physical visits to government offices. This accessibility ensures equitable service delivery and enhances citizen satisfaction.

VI. Data-Driven Decision Making: E-governance models leverage data analytics and business intelligence tools to inform decision-making processes. By analyzing large datasets on demographics, socio-economic indicators, and citizen feedback, governments can identify trends, prioritize interventions, and allocate resources more effectively. Data-driven decision-making enhances the efficiency and effectiveness of governance strategies.

VII. Innovation and Modernization: E-governance fosters innovation and modernization in government operations by embracing emerging technologies and best practices. By investing in digital infrastructure, cybersecurity measures, and skill development, governments can build resilience, adaptability, and competitiveness in the digital age. Innovation-driven governance promotes continuous improvement and responsiveness to evolving citizen needs.

In conclusion, e-governance models offer transformative opportunities to enhance good governance principles by promoting transparency, efficiency, accountability, citizen engagement, access to services, data-driven decision-making, and innovation

8. **What are the issues related to E governance application? Why do we need to consider these issues?**

Ans:

There are several key issues that need to be considered when implementing e-governance applications. These include:

Digital Divide:

- The unequal access to digital technologies and the internet across different socioeconomic groups can create a digital divide, excluding certain segments of the population from e-governance services.
- This needs to be addressed to ensure equitable access and participation.

Cybersecurity and Data Privacy:

- The increased digitization of government data and services raises concerns about cybersecurity threats and the protection of sensitive personal and citizen information.

- Robust security measures and data privacy safeguards are crucial to build public trust in e-governance.

Interoperability and Integration:

- Effective e-governance requires seamless integration and interoperability between different government IT systems and databases.
- Addressing technical, organizational, and semantic barriers to integration is essential for the successful implementation of e-governance.

Capacity Building and Digital Literacy:

- Governments need to invest in building the digital skills and capabilities of both public officials and citizens to enable effective utilization of e-governance services.
- Addressing the digital literacy gap is necessary for the successful adoption and sustained use of e-governance applications.

Change Management and Resistance to Change:

- The transition from traditional, paper-based governance to digital e-governance can face resistance from within the government bureaucracy and among citizens.
- Effective change management strategies, including stakeholder engagement and communication, are required to facilitate the cultural shift.

Sustainability and Scalability:

- Ensuring the long-term sustainability and scalability of e-governance initiatives is crucial, as they often require significant upfront investments in infrastructure and ongoing maintenance.
- Addressing funding, governance, and technological challenges is essential for the scalability and sustainability of e-governance projects.

Ethical and Legal Considerations:

- E-governance raises ethical questions around data use, algorithmic decision-making, and the potential for algorithmic bias.

- Developing and enforcing appropriate legal and regulatory frameworks is necessary to address these ethical concerns and ensure responsible and accountable e-governance.

By considering and addressing these issues, governments can develop and implement e-governance applications that are inclusive, secure, interoperable, scalable, and aligned with the principles of good governance. Failing to address these challenges can undermine the effectiveness and public trust in e-governance initiatives, hindering their ability to drive transformative change in the public sector.

9. **What are the various Security Approaches for E-Government?**

Ans:

The various Security Approaches for E-Government are explained below:

Access Control:

- Implementing access control mechanisms to restrict unauthorized access to government systems and data.
- This includes user authentication methods such as passwords, biometrics, and multi-factor authentication to verify the identity of users accessing government resources.

Network Security:

- Deploying firewalls, intrusion detection/prevention systems, and virtual private networks (VPNs) to secure the communication channels and network infrastructure.
- This helps to mitigate external cyber threats and prevent unauthorized access to e-government systems.

Application Security:

- Securing the e-government applications and web portals by implementing secure coding practices, input validation, and protection against common web application vulnerabilities.
- This safeguards the applications from potential exploitation and data breaches.

Security Monitoring and Audit:

- Implementing robust security monitoring, logging, and auditing mechanisms to detect and respond to potential security breaches or anomalous activities.
- This provides visibility into the security posture and enables compliance with relevant regulations and standards.

Cybersecurity Awareness and Training:

- Educating and training government employees and citizens on cybersecurity best practices, such as password management, phishing awareness, and secure online behavior.
- This helps to reduce the risk of human-related security vulnerabilities.

Patch Management:

- Regularly updating and patching software, operating systems, and applications to address known security vulnerabilities and mitigate the risk of exploitation by attackers.
- Patch management helps ensure that e-government systems remain secure and resilient against emerging threats.

10. Write short note on Ekal Seva Kendra.

Ans: Ekal Seva Kendra, established at the district secretariat in Kaithal, Haryana, is a pioneering initiative aimed at providing people-friendly, need-based governance through a comprehensive service delivery model. With a mission to offer

time-bound, hassle-free services in a professional and citizen-friendly environment, Ekal Seva Kendra operates under the following objectives:

i. Time-bound Delivery: Ensuring prompt delivery of services to citizens within stipulated timeframes.
ii. Single-point Contact: Providing a centralized location for accessing multiple government services under one roof.
iii. Simplified Procedure: Implementing transparent and simplified procedures for service delivery, ensuring total transparency.
iv. Easy Monitoring and Accountability: Facilitating easy monitoring and establishing fixed accountability for service delivery.
v. Total Solution: Offering integrated computerized solutions for all service-related activities.
vi. Elimination of Bogus Licenses: Preventing the issuance of fake licenses through tamper-proof databases and rigorous scrutiny.
vii. Reduced Clerical Workload: Streamlining processes to reduce administrative burdens and enhance efficiency.
viii. Self-sustained Project: Ensuring the sustainability of the project through funding from the District Red Cross Society and user contributions.

Technologically, Ekal Seva Kendra utilizes versatile and robust software developed by the National Information Centre, featuring Visual Basic and SQL Server technologies for front-end and back-end operations, respectively. The system employs a server with seven nodes and various printers connected through a local area network, ensuring connectivity with relevant government offices.

Operational aspects include the implementation of software solutions like Sarathi for driving license issuance, Vahan for vehicle registration, Certificate for various certificate issuance, Nakal for revenue document services, and Passport for passport application processing. These software modules facilitate efficient service delivery, online security, and generation of management information system (MIS) reports.

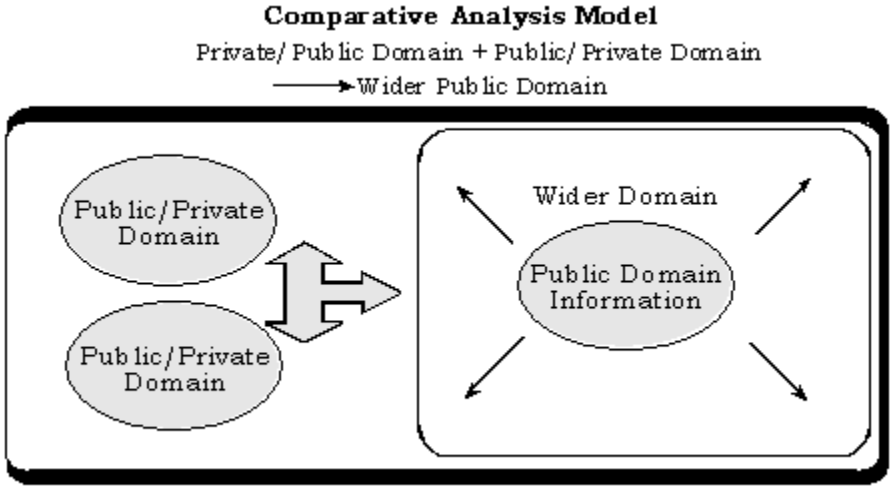
Moreover, Ekal Seva Kendra maintains self-sustainability by covering all operational expenses, including manpower, through funding from the District Red Cross Society and nominal service charges levied on users. These charges cover expenses such as blood group tests, government forms, photographs, and document lamination.

In summary, Ekal Seva Kendra represents a paradigm shift in governance, leveraging technology, transparency, and citizen-centricity to deliver efficient and accessible government services, thereby fostering good governance principles at the grassroots level.

11. Define Comparative Analysis Model with proper application and diagram.

Ans:

The Comparative Analysis Model is one of the five main e-governance models. It focuses on using information and best practices from other governments or organizations to improve local governance practices. This model emphasizes learning from successful e-governance implementations elsewhere and adapting those practices to the local context. It involves systematically analyzing and comparing various aspects of e-government implementation and service delivery to identify best practices, areas for improvement, and opportunities for optimization.



The Comparative Analysis Model can be applied in the following ways to support e-governance initiatives:

1. Benchmarking E-Government Services:

- Comparing the quality, accessibility, and user satisfaction of e-government services across different agencies or jurisdictions.
- This helps identify high-performing e-government services and share best practices.

2. Evaluating E-Government Initiatives:
    - Assessing the implementation, adoption, and impact of specific e-governance initiatives, such as digital service delivery, online citizen engagement platforms, or back-end system modernization.
    - The comparative analysis can inform decision-making and guide future e-government investments.
3. Analyzing E-Government Performance:
    - Comparing the overall performance, efficiency, and effectiveness of e-government systems and processes across different government entities.
    - This can include metrics such as cost savings, process streamlining, citizen satisfaction, and transparency.
4. Identifying Areas for Improvement:
    - Pinpointing specific areas where certain government agencies or jurisdictions are underperforming compared to their peers.
    - This can help prioritize and target interventions to enhance the quality and delivery of e-government services.