Long Answer Questions:
Attempt any TWO Questions:

1. Discuss in brief about E-Governance in China.

   E-Governance in China

   Introduction

   E-government has made good achievements in China and played a major role in improving administrative institutions and provision of public services. In China, the applications of e-government increased since 2001. The application of e-government in China was intended, in part, to accelerate the government's pace of implementing and using information and communications technologies (ICTs) to improve administrative efficiency and effectiveness and, through this administrative reform, to promote economic development and the administrative capacity (Hongguan Tiaokong Nengli) of the central government in China. While Chinese leaders also emphasize the importance of providing a better quality of public services to their citizens, the major goal of e-government seems to be interestingly different than in western countries. Some critical problems have arisen at the same time as in many other developing countries, such as institutional inertia, over expenditure, lack of use, lack of knowledge, lack of infrastructure, asymmetry of regional development, etc. China should consider formulating effective e-government policy as well as creating an institutional mechanism in various government departments for integrating and sharing e-government applications across provinces and local governments. This could prove especially helpful to those citizens who are living in the less developed regions and provinces lacking e-government delivery of public services.

   In China, the focus of e-government has mainly been on administrative reform (Xingzheng Guanli Tizhi Gaige) which has to enter into other areas. As a consequence of a deeply centralized and often inefficient administrative management system, China has faced critical problems including over bloated structures, overstaffing, confusion between government and enterprise management, and the often unhelpful intervention of the central government in the economy (Lianjie, Chung & Thorson, 2005).

   The application of e-government in China was intended, in part, to accelerate the government's pace of implementing and using information and communications technologies (ICTs) to improve administrative efficiency and effectiveness and, through this administrative reform, to promote economic development and the administrative capacity (Hongguan Tiaokong Nengli) of the central government in China (Lianjie, Chung & Thorson, 2005).

   In an age of information expansion, the Chinese government has actively encouraged and invested in the growth of the Internet to capture the technology's vast commercial potential while exerting state control over the ways that this "network of networks" is accessed by Chinese citizens. The central government has encouraged the competing state-owned telecommunications providers, such as China Telecom, China Unicom, China Mobile, China Netcom, JiTong Communications Company, and China Railway Telecom, to build their own networks. Faced with the potential political or social challenges that the new medium may

bring, the Chinese Communist Party (CCP) has utilized multiple control strategies to maximize official authority.

The Hi-tech E-park

The Zhongguanccun Science Park (ZSP), the biggest National Science Park in China was established in 1988, in the North-Western part of Beijing City, the capital of People's Republic of China.

The Park spans over 100 square kilometers comprising of more than 600 companies in Hi-tech areas as IT, Biology, Medicine, etc. Large multinationals such as IBM, Microsoft, Lucent, HP, and Epson have thri R & D institution here. Thirty-nine prominent universities and colleges such as Beijing University and Tsinghua University are also located within the park.

The ZSP Administrative committee which is the local government body that regulates, controls and administers all activities in the park has twelve departments, each looking after functions as Company Certification, Taxation and the like.

The administration of the park formed a strategic partnership with a local private application software company, Beijing Beauty Bearrl limited which started the system study and completed the software development by the end of the year 2000.

In the new system the central database and web site allow data sharing and workflow integration among all the departments. Thus the administration functions are a single integrated body showing only one face to the public. The system includes five functions, all accessed from the web site homepage of the web site.

Major Functions:

The following are the five functions of the system.

1. **E-application**

    This is a web based software that provides the applicants with all form and documents required, along with rules and regulations, and also procedure for setting up a company in the Park. After login with the user ID and password the users can fill up the files directly on the web or download the forms, fill them up on the computer, and upload them into the web. The form will depend upon the nature of the company. Almost instantaneously, the ZSP Administration committee receives the applications and beings approval procedures online. Two or three layers of approval are processed by the Administration. In each layer the Administration sends its comments/feedback/objectives to the company online. The company will make corrections online and submit immediately.

    This process of submitting, correcting and resubmitting will proceed until the final approval is granted online. The applicant company will then take a printout of the approval file and submit all the original documents to ZSP verification, the license certificate will be issued to the applicant.

    As can be seen above only once there is a physical visit by the applicant to the administration office, i.e. for the final approval. Till then all the steps are automatically online.

2. **E-Registration**

    After obtaining approval for establishing the company, additional information is required to be provided to the administration in order to register with other department of ZSP. e.g. Statistical Bureau, Finance Bureau and Quality Control Bureau. All these now can be done through Internet.

3. E-Reporting

Every company has to report every month to the ZSP administrations and other appropriate governments offices various information parameters such as the company revenue, tax, costs, cash flow, etc. All these can now be done online.

4. E-Administrations

Other administrative information leading to tax cut, tax assessment, and subsidiaries, are all calculated on the web in the new systems. Financial and other information also will be submitted by the companies online.

5. E-Consulting

Government official can provide online interactive consultation regarding any of these procedures, and replies can be sent by Fax and Email.

Benefits:

A very impressive benefits list of the system can be made. Since operationalization in August 2000 several hundred thousand people have visited up to 5000. Several thousands of companies' license and approvals of various kinds have been issued through the systems. They have all submitted their financial returns through the online web based system. Other benefits are, transparency, speed, and efficiency, added to interactive, session.

2. Explain E-Government as Information System with proper diagram.

3. Compare and contrast Wider dissemination and Critical Flow Model.

Section "B"

Short Answer Questions:

1. Explain Biba model. How does it differs from Bell la Padula model?

   Biba Integrity Model

   The Biba model is a formal security model named after its creator, Kenneth J. Biba, introduced in 1977. It primarily focuses on integrity rather than confidentiality, although it can be used in conjunction with other models to provide comprehensive security. The Biba model is particularly useful in environments where data integrity is of utmost importance, such as financial systems, critical infrastructure, and healthcare.

   - Similar to the Bell-LaPadula model's security levels, the Biba model defines integrity levels for both subjects (users or processes) and objects (resources or data).
   - Integrity levels are often represented as labels and typically follow a hierarchical structure, such as "Low," "Medium," and "High."
   - The Simple Integrity Property (no read-down) states that a subject at a certain integrity level should not read data from objects at a lower integrity level.
   - The Star Integrity Property (no write-up) states that a subject at a certain integrity level should not write data to objects at a higher integrity level.
   - The Biba model also includes a concurrency property, which ensures that subjects with the same integrity level cannot concurrently modify objects to maintain the integrity of the system.

2. What are the five maturity models in E governance?

   Five Maturity Models of E-Governance

   The Five Maturity Levels

3. Explain Human Infrastructural Preparedness.

Human Infrastructural Preparedness

Human infrastructural preparedness refers to the readiness of individuals, organizations, or communities to effectively utilize and manage human resources for achieving specific goals or addressing challenges. In the context of governance, human infrastructural preparedness is essential for ensuring that individuals possess the necessary skills, knowledge, and capacities to participate in and contribute to governance processes effectively.

Components of Human Infrastructural Preparedness:

- **Capacity Building:** Providing training, education, and skill development programs to enhance the capabilities of government officials, civil servants, and citizens in areas such as policy analysis, decision-making, project management, and communication.
- **Leadership Development:** Cultivating leadership skills among government leaders and administrators to effectively manage change, inspire innovation, and promote accountability and transparency in governance.
- **Citizen Engagement:** Promoting active citizen participation in governance processes through awareness-raising campaigns, civic education initiatives, and platforms for public dialogue and feedback.
- **Ethical and Professional Standards:** Instilling values of integrity, professionalism, and ethical conduct among public servants to uphold the public trust and maintain high standards of governance.
- **Diversity and Inclusion:** Promoting diversity and inclusiveness in decision-making processes and ensuring the representation of marginalized groups and underprivileged communities in governance structures.

4. Explain Online Service Delivery and Electronic Service Delivery with proper example.

Online Service Delivery (OSD):

OSD specifically emphasizes the delivery of government services through online channels. It highlights the use of the internet and web-based platforms to provide services to citizens, businesses, and other government entities.

Characteristics:

- **Web-based Platforms:** OSD relies on websites, portals, and other online platforms where users can access and interact with government services.
- **Internet Accessibility:** The emphasis is on making services accessible to users with internet connectivity, often through personal computers, laptops, or mobile devices.
- **User-Friendly Interfaces:** OSD platforms aim to provide user-friendly interfaces for citizens to easily navigate and complete transactions or access information.

Electronic Service Delivery (ESD):

ESD is a broader term that encompasses the use of electronic means, not limited to online platforms, to deliver government services. It includes various electronic channels and technologies beyond the internet.

Characteristics:

- **Multichannel Approach:** ESD recognizes that service delivery can occur through various electronic channels, including but not limited to online platforms. This may include mobile applications, telephone services, SMS, and other electronic methods.

- **Integration of Technologies:** ESD involves the integration of different electronic technologies to provide a seamless experience for users. This may include electronic forms, automated phone systems, and other electronic interfaces.
- **Accessibility Through Diverse Platforms:** While online channels are part of ESD, the focus is on providing services through diverse electronic platforms to reach a broader audience.

5. What is Data Mining? Explain Applications of data mining.
Data Mining

Salient Features
Applications:

6. Difference between E government and E governance.

7. Write a short note on E seva.
E-Seva

e-Seva in Andhra Pradesh, Friends in Kerala, Sukhmani centres in Punjab, the Lok-Mitra project in Rajasthan, Coimbatore-Online in Tamil Nadu and Bangalore One in Karnataka are some of the pioneering G2C initiatives in India. It is one of the e-governance initiatives, officers a wide spectrum of citizen friendly service to save citizen the trouble of running around various departments.

e-Seva has several innovations to its credit. The people interface issue has been well addressed and the effects of re-engineering are there for all to see. The ambience is good, the place is clean, less noisy and there is an air-conditioned environment, uncluttered by dilapidated furniture. There is access to drinking water, facilities like ATM, internet kiosks and phones, things one does not normally associate with government departments in India. The services are offered at dozens of centres, each with several counters, in a public-private-partnership model. The computers, printers and internet access are provided by the private operator, who is paid a fixed service charge for transactions completed at e-Seva counters, with the government providing the data.

Salient Features:
Following are the salient features of e-seva:
- Provides real time online transactions.
- Integrated Citizen Service Centres (ICSCs) operates from 8 a.m to 8 p.m. on all working days and is open on Sundays and Second Saturdays also 9.00 a.m. to 3:00 p.m.
- Electronic queuing system and efficient transaction of business reduces waiting time.
- Distribution of centre in all major areas surrounding the city, likely to expand to other parts of the State also.

Implementation Model-Public Private Partnership

This project has been implemented to a Public-Private Partnership model. The technology is based on a 3-tier architecture. The transactions are done on a real-time basis. The servers of different departments are connected to the e-Seva Data Centre, which is in turn connected to different ICSCs. The connectivity is provided through leased lines with ISDN line as backup. Transactions conducted at the ICSCs are recorded directly on the server of the department concerned, after duly according the same in the central server.

Each ICSC has 10-14 computerized manned counter with one PC, printer, bar-code reader per counter to handle the services.

Service Centres:

At present, there are 46 e-Seva centres spread across the twin cities of Hyderabad and Secunderabad and Rana Reddy District, and two bank branches of Andhra Bank and State Bank of Hyderabad respectively.

Extension to Districts:

Regarding the replication of e-sewa in municipalities in the Stage, it was decided to expand the e-Seva services in all 117 municipalities in the state, which cover 85% of the population of the state.

Conclusion:

In this case study on e-seva of Andhra Pradesh Government, we surveyed the salient features, details of services offered and proposed future services E-Sava is the most successful among all projects in India that have reached common man with essential services of the Government. Municipality and also Utility Companies all under one roof.

8. What are the Challenges and Approach of E-government Security?

E-Government:

E-government, or electronic government, refers to the use of information and communication technologies (ICTs) to enhance the efficiency, effectiveness, and transparency of government services and processes. Ensuring the security of e-government systems is crucial to safeguarding sensitive information, maintaining public trust, and preventing cyber threats.

Challenges:

- **Cybersecurity Threats:** E-government systems face a wide range of cyber threats, including malware, phishing attacks, ransomware, and distributed denial-of-service (DDoS) attacks. These threats can disrupt services, steal sensitive data, or compromise the integrity of government systems.
- **Data Privacy:** E-government platforms often handle large amounts of personal and sensitive information. Ensuring the privacy and confidentiality of this data is essential to protect citizens' rights and prevent identity theft or unauthorized access.
- **Complexity of Systems:** E-government initiatives typically involve complex systems and interconnected networks, making them vulnerable to security vulnerabilities and misconfigurations. Managing security across these diverse systems can be challenging, especially when integrating legacy systems with newer technologies.
- **Insider Threats:** Insider threats, whether intentional or accidental, pose a significant risk to e-government security. Employees or contractors with privileged access to government systems may abuse their privileges, leak sensitive information, or inadvertently introduce security vulnerabilities.
- **Compliance and Regulations:** E-government initiatives must comply with various regulations and standards related to data protection, privacy, and cybersecurity. Ensuring compliance with these requirements adds complexity to security management and may require substantial resources.

Approaches:

- **Risk Assessment and Management:** Conducting regular risk assessments helps identify potential security threats and vulnerabilities within e-government systems. By prioritizing risks and implementing appropriate controls, government agencies can mitigate security risks effectively.

- **Security by Design:** Implementing security measures from the design phase of e-government projects helps build robust security foundations. This includes incorporating security features such as encryption, access controls, and authentication mechanisms into system architecture and development processes.
- **Access Control and Authentication:** Implementing strong access control measures, such as role-based access control (RBAC) and multi-factor authentication (MFA), helps prevent unauthorized access to government systems and sensitive data.
- **Continuous Monitoring and Incident Response:** Adopting continuous monitoring tools and practices allows government agencies to detect security incidents promptly and respond effectively. Establishing incident response plans and conducting regular security drills help ensure a rapid and coordinated response to cyber threats.
- **Education and Training:** Providing cybersecurity awareness training to government employees and contractors helps raise awareness about security best practices and reduces the risk of insider threats. Training programs should cover topics such as phishing awareness, secure password management, and data handling procedures.