Project proposal for

**Finger Print Based ATM System**

|  |  |  |
| --- | --- | --- |
|  | Member ID | Member Name |
| Group No | 19-41342-3 | Md. Ahsanul Mostakin |
| 09 | 20-42585-1 | Saiful, Islam |
| 20-42447-1 | Mouri Kamal |

[Date]

A picture containing text, logo, circle, trademark

Description automatically generated

Ahsanul Mostakin

**Software Project Proposal**

**Client**: ABC Banking

**Contact Person**: Jhony Islam

**Address**: C Block Main Street, Bashundhara, Dhaka 1229

**Date**: November 16, 2023

**Service Provider**: Web Dynamics

**Introduction**

Web Dynamics is an IT company specializing in software development. We have a proven track record of providing customized software solutions to businesses of all sizes across various industries. Our team of experienced developers and consultants is committed to understanding our clients' unique needs and delivering high-quality software that meets their specific requirements.

**Overview of the proposed system**

ABC Banking has approached Web Dynamics to develop a new core banking system to streamline its operations, enhance customer service, and improve overall efficiency. The proposed system will encompass a comprehensive suite of functionalities, including:

* Account management
* Transaction processing
* Loan origination and servicing
* Customer relationship management (CRM)
* Regulatory compliance reporting

**Objectives and subobjectives**

The primary objectives of the proposed core banking system are to:

1. **Modernize the bank's IT infrastructure**: Replace outdated legacy systems with a modern, scalable, and secure platform.
2. **Improve operational efficiency**: Automate manual processes, reduce errors, and streamline workflows to enhance productivity.
3. **Enhance customer experience**: Provide customers with self-service capabilities, personalized banking services, and improved access to information.
4. **Strengthen regulatory compliance**: Ensure adherence to all applicable regulations and reporting requirements.

To achieve these objectives, the system will be designed to meet the following sub-objectives:

1. **Account management**: Create and manage customer accounts, including account types, transactions, statements, and alerts.
2. **Transaction processing**: Process various types of transactions, such as deposits, withdrawals, transfers, and payments.
3. **Loan origination and servicing**: Manage the entire loan lifecycle, from application to disbursement, collection, and reporting.
4. **CRM**: Maintain and manage customer relationships, track interactions, and provide personalized services.
5. **Regulatory compliance reporting**: Generate reports and meet compliance requirements for various regulations.

**Justifications**

The proposed core banking system is justified by the following benefits:

* **Improved operational efficiency**: The system will automate manual processes, reduce errors, and streamline workflows, leading to increased productivity and cost savings.
* **Enhanced customer experience:** Customers will benefit from self-service capabilities, personalized banking services, and improved access to information, leading to increased satisfaction and loyalty.
* **Strengthened regulatory compliance:** The system will ensure adherence to all applicable regulations and reporting requirements, mitigating risks and legal liabilities.
* **Competitive advantage:** The adoption of a modern, scalable core banking system will position ABC Banking at the forefront of technological innovation, giving it a competitive edge in the industry.

Web Dynamics is confident that our expertise and experience in developing core banking systems make us the ideal partner for ABC Banking. We are committed to working closely with ABC Banking to understand its specific requirements and deliver a high-quality software solution that meets its business objectives. We are confident that the proposed core banking system will deliver significant benefits to ABC Banking, enabling it to achieve its strategic goals and enhance its overall performance.

**Use case Diagram**

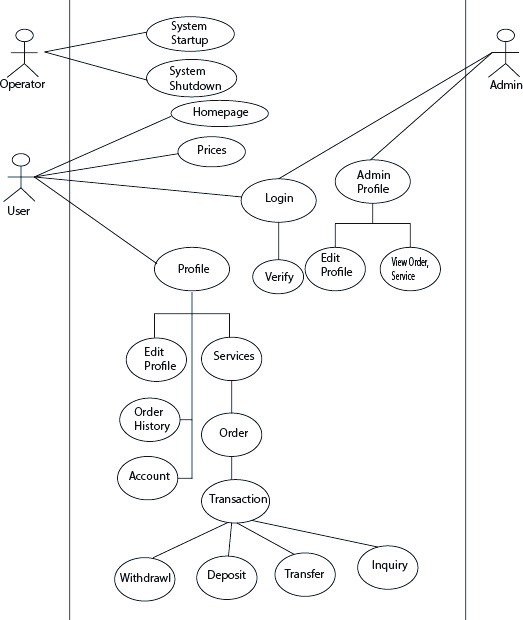
****

Fig: Use Case Diagram

**Project Scope and features**:

**Project Scope:**

The scope of a fingerprint-based ATM system involves the various aspects and functionalities that the project aims to encompass. Here are the key scopes or components of a fingerprint-based ATM system:

* **Biometric Enrollment and Authentication:**
  + Develop a system for capturing and storing the fingerprints of users during the enrollment process.
  + Implement a robust biometric authentication system that verifies the user's identity based on their fingerprint.
* **Integration with the Core Banking System:**
  + Integrate the fingerprint-based authentication system seamlessly with the core banking system to ensure real-time account verification and transaction processing.
* **Security Measures:**
  + Implement advanced security measures, such as encryption and secure protocols, to protect the biometric data and ensure that the system is resistant to unauthorized access.
* **Multi-Factor Authentication:**
  + Consider implementing multi-factor authentication, combining fingerprint recognition with other factors like PINs or one-time passwords for enhanced security.
* **Transaction Authorization:**
  + Enable users to perform various financial transactions (withdrawals, deposits, fund transfers) using their fingerprints as the primary means of authorization.
* **User Interface Design:**
  + Design an intuitive and user-friendly interface on the ATM to guide users through the fingerprint enrollment and authentication processes.
* **Anti-Spoofing Measures:**
  + Integrate anti-spoofing measures to prevent fraudulent attempts, such as using fake fingerprints.
* **Database Management:**
  + Establish a secure database management system to store and manage the biometric data of authorized users.
* **Compliance with Regulations:**
  + Ensure compliance with relevant regulations and standards related to biometric data storage, user privacy, and data protection laws.
* **Testing and Quality Assurance:**
  + Conduct thorough testing to validate the accuracy, speed, and reliability of the fingerprint recognition algorithm and overall system performance.
* **Logging and Auditing:**
  + Implement logging mechanisms to record all transactions and authentication attempts for auditing and security purposes.
* **User Education and Training:**
  + Provide user training to familiarize individuals with the new fingerprint-based authentication system and educate them on its benefits and security features.
* **Maintenance and Support:**
  + Establish a maintenance plan to address any issues that may arise post-implementation and provide ongoing support to ensure the system's reliability.
* **Hardware Integration:**
  + Integrate fingerprint scanning hardware with the ATM system, ensuring compatibility and reliability.
* **Emergency Protocols:**
  + Develop protocols for handling emergencies, such as system failures, to ensure user safety and continuity of services.
* **Transaction Limits and Controls:**
  + Implement controls and limits on transactions to prevent misuse and enhance security.
* **User Privacy Protection:**
  + Implement measures to protect user privacy and communicate the privacy features of the fingerprint-based ATM system.

By addressing these project scopes, a fingerprint-based ATM system can offer a secure, convenient, and efficient means of user authentication and financial transactions. The successful implementation of these scopes contributes to the overall success and acceptance of the system by users and regulatory authorities.

**Features:**

The features of an ATM (Automated Teller Machine) system can vary based on the specific implementation and technology used. However, here are some common features that you might find in a typical ATM system:

* **Cash Withdrawal:**
  + Users can withdraw cash from their bank accounts using their debit or credit cards.
* **Balance Inquiry:**
  + Users can check the balance of their bank accounts to know how much money is available.
* **Cash Deposits:**
  + Some ATMs allow users to deposit cash into their accounts, providing a convenient way to add funds.
* **Check Deposits:**
  + In addition to cash, some ATMs accept check deposits, allowing users to deposit checks directly into their accounts.
* **Fund Transfers:**
  + Users can transfer money between their accounts or to other accounts within the same bank.
* **PIN Change:**
  + Users can change the Personal Identification Number (PIN) associated with their ATM card for security purposes.
* **Mini Statements:**
  + Users can request a mini statement that provides a summary of recent transactions on their accounts.
* **Mobile Recharge:**
  + Some ATMs allow users to recharge their mobile phones or pay utility bills directly through the ATM interface.
* **Cardless Transactions:**
  + Users may have the option to perform transactions without physically inserting their card, using methods such as mobile banking apps or QR codes.
* **Language Selection:**
  + ATMs often support multiple languages, allowing users to choose their preferred language for the transaction interface.
* **Receipt Printing:**
  + A transaction receipt is typically provided to users for their records.
* **Touchscreen Interface:**
  + Many modern ATMs feature touchscreen interfaces for a more user-friendly experience.
* **Contactless Transactions:**
  + Some ATMs support contactless card transactions or Near Field Communication (NFC) for enhanced convenience and speed.
* **Accessibility Features:**
  + ATMs should be designed to be accessible to people with disabilities, with features such as voice guidance, Braille instructions, and lower-height interfaces.
* **Security Features:**
  + Security measures include PIN-based authentication, card skimming detection, and surveillance cameras to ensure user safety.
* **Remote Monitoring:**
  + ATMs are often remotely monitored to detect any issues or suspicious activities.
* **Emergency Services:**
  + ATMs may have an emergency button or feature to contact the bank or emergency services in case of any issues.
* **Currency Conversion:**
  + For international travelers, some ATMs provide the option to withdraw cash in the local currency.
* **Customer Support Information:**
  + Contact information for customer support or the bank's helpline is usually displayed on the ATM interface.
* **Transaction Security Alerts:**
  + Users may receive alerts (via SMS or email) for significant transactions to enhance security.

These features collectively aim to provide users with a range of convenient and secure financial services through the ATM system.

**Primary and Secondary Stakeholders:**

**Primary Stakeholders:**

* **Users:**
  + Users of the ATM system are primary stakeholders as they directly interact with and benefit from the system. They are interested in a secure, convenient, and efficient means of accessing their accounts and conducting financial transactions using fingerprint authentication.
* **Financial Institution/Bank:**
  + The bank or financial institution deploying the fingerprint-based ATM system is a key stakeholder. They are interested in the project's success in terms of enhancing security, improving customer experience, and ensuring compliance with regulatory standards.
* **Project Team:**
  + The project team responsible for designing, developing, testing, and implementing the fingerprint-based ATM system is a primary stakeholder. This includes project managers, developers, engineers, and other team members.
* **Biometric Technology Providers:**
  + Companies or vendors providing biometric technology, including fingerprint recognition algorithms and hardware components, are crucial stakeholders. The success of the project reflects the success of their technology.
* **Regulatory Authorities:**
  + Regulatory bodies overseeing banking and biometric data usage are primary stakeholders. The project must comply with regulations to ensure the legal and ethical use of biometric data, protecting user privacy and security.

**Secondary Stakeholders**

* **Government Agencies:**
  + Government agencies at various levels may have an interest in the project, especially if it involves compliance with national or regional regulations, standards, or initiatives related to technology and financial services.
* **Technology Partners:**
  + Companies providing other technological components, such as networking infrastructure, software frameworks, or security solutions, are secondary stakeholders.
* **Security Auditors:**
  + External security auditors or firms conducting audits on the system's security features and data protection measures are secondary stakeholders.
* **Local Communities:**
  + The local communities where the ATMs are deployed may be secondary stakeholders, as the project can impact the accessibility of banking services in those areas.
* **Consumer Advocacy Groups:**
  + Groups advocating for consumer rights and data privacy may have an interest in ensuring that the fingerprint-based ATM system is designed and implemented with the utmost consideration for user privacy and security.
* **ATM Maintenance and Service Providers:**
  + Companies responsible for the maintenance and servicing of ATMs are secondary stakeholders. They are interested in the reliability and ease of maintenance of fingerprint-based ATMs.
* **Insurance Companies:**
  + Insurance companies may have an interest in the project, particularly if it affects the risk and security landscape of financial transactions.

Understanding and managing the interests and expectations of both primary and secondary stakeholders is essential for the successful planning, development, and deployment of a fingerprint-based ATM system. Regular communication, collaboration, and addressing the concerns of these stakeholders contribute to the overall success of the project.

**Technical Requirements:**

**Operating Systems:**

The operating systems involved in a fingerprint-based ATM system project can depend on the specific technology stack chosen by the developers and the requirements of the system. Here are some possible operating systems that might be involved:

* **Embedded System OS:**
  + Many ATMs use embedded operating systems tailored for specific hardware configurations. Examples include Windows Embedded, Linux-based systems (e.g., Embedded Linux), or custom proprietary operating systems designed for ATMs.
* **Windows OS:**
  + Some ATMs run on various versions of the Windows operating system. Windows 7, Windows 10 IoT (Internet of Things), or Windows Server editions may be utilized.
* **Linux OS:**
  + Linux is a common choice for embedded systems, and certain ATMs may run on Linux-based operating systems. Examples include distributions like Ubuntu, CentOS, or custom Linux configurations.
* **Real-Time Operating System (RTOS):**
  + RTOS may be used for tasks requiring precise timing and quick responses, enhancing the security and performance of the fingerprint recognition system. Examples include FreeRTOS or QNX.
* **Mobile Operating Systems:**
  + If the ATM incorporates mobile features or interfaces with mobile devices, the project might involve aspects of mobile operating systems like Android or iOS.
* **Database Management System (DBMS):**
  + While not an operating system in the traditional sense, the choice of a database management system is crucial. Examples include Microsoft SQL Server, MySQL, or PostgreSQL for managing user data and transaction records.
* **Biometric Software Stack:**
  + The fingerprint recognition system may include specialized software for biometric data processing. This could run on an operating system that supports the necessary libraries and drivers.
* **Networking and Security Operating Systems:**
  + For managing network connections, security protocols, and firewalls, there might be elements of operating systems focused on these aspects, such as specialized network security appliances.
* **ATM Controller Software:**
  + ATMs typically have a controller unit with software managing the overall operation of the ATM. This software may run on a specific operating system designed for ATM control.

The specific choice of operating system depends on factors like system requirements, hardware compatibility, security considerations, and the preferences of the developers or the financial institution deploying the ATM system. The operating systems mentioned above are examples, and the actual selection may vary based on the project's technical specifications and goals.

**Implementing Software Requirements:**

Implementing software requirements in a fingerprint-based ATM system project involves creating the necessary software components to meet the specified functional and non-functional requirements. Here are key aspects of the software implementation for such a project:

* **Biometric Enrollment Software:**
  + Develop software to capture and store fingerprint data during the user enrollment process. This software ensures accurate and secure storage of biometric information associated with user accounts.
* **Fingerprint Recognition Algorithm:**
  + Implement a robust fingerprint recognition algorithm that is capable of accurately matching enrolled fingerprints during the authentication process. This algorithm is a critical component of the biometric authentication system.
* **Integration with Core Banking System:**
  + Develop software interfaces and protocols to integrate the fingerprint-based ATM system with the core banking system. This includes communication protocols to retrieve account information, process transactions, and update account balances.
* **User Interface (UI) Design:**
  + Create an intuitive and user-friendly software interface for the ATM. The UI should guide users through the fingerprint enrollment and authentication processes and provide a seamless experience for conducting transactions.
* **Transaction Processing Software:**
  + Develop software modules for processing various financial transactions such as cash withdrawals, deposits, fund transfers, and balance inquiries. This software interacts with the core banking system to execute these transactions securely.
* **Security Software:**
  + Implement security features, including encryption algorithms, secure communication protocols, and measures to protect against unauthorized access. This software is crucial for safeguarding user data and transaction information.
* **Multi-Factor Authentication Software:**
  + If the system incorporates multi-factor authentication, develop software to manage the combination of fingerprint recognition with other factors like PINs or one-time passwords.
* **Anti-Spoofing Measures:**
  + Implement software-based anti-spoofing measures to detect and prevent fraudulent attempts, such as using fake fingerprints or other biometric spoofing techniques.
* **Database Management Software:**
  + Choose and implement a database management system (DBMS) to securely store and manage user account information, transaction records, and biometric data.
* **Logging and Auditing Software:**
  + Develop software modules for logging all system activities, including user transactions, authentication attempts, and system events. This supports auditing, monitoring, and forensic analysis.
* **Software for Remote Monitoring and Maintenance:**
  + Implement software solutions for remote monitoring of ATMs, enabling real-time tracking of system health, status, and security. This facilitates proactive maintenance and issue resolution.
* **Error Handling and Recovery Software:**
  + Develop software components for error handling and recovery mechanisms to ensure system stability and reliability in case of unexpected events or errors.
* **Notification Software:**
  + Implement software to generate and send notifications, such as transaction alerts, to users for significant events or changes in their accounts.
* **Update and Patch Management Software:**
  + Implement a system for managing software updates and patches to ensure that the ATM system remains up to date with the latest security enhancements and features.
* **Mobile Integration Software (if applicable):**
  + If the ATM system integrates with mobile devices, develop software components for seamless communication and data exchange between the ATM and mobile platforms.
* **Compliance Software:**
  + Implement software solutions to ensure compliance with regulatory requirements, data protection laws, and industry standards.

The successful implementation of these software requirements ensures the reliable, secure, and user-friendly operation of a fingerprint-based ATM system. The software components need to work seamlessly together to provide a robust and efficient banking experience for users.

**Hardware Requirements:**

The hardware requirements for a fingerprint-based ATM system project involve the physical components necessary for the system to function. Here are key hardware components that are typically involved in such a project:

* **ATM Hardware**:
  + The core hardware includes the ATM itself, which comprises a secure enclosure, a display screen, a PIN pad, a cash dispensing mechanism, deposit slots, and other physical components that make up the ATM structure.
* **Biometric Hardware**:
  + Fingerprint scanning hardware is crucial for capturing and verifying the biometric information of users. This hardware includes fingerprint sensors capable of high-quality image capture for accurate authentication.
* **Secure Enclosure**:
  + The ATM should be housed in a secure enclosure to protect the internal components from physical tampering or unauthorized access.
* **Card Reader**:
  + Although the emphasis is on fingerprint authentication, the system may still include a card reader for situations where additional verification methods are required, or in cases where the user does not use fingerprint authentication.
* **Cash Dispensing Mechanism**:
  + The hardware responsible for dispensing cash includes secure cassettes or dispensers to hold and release currency notes based on user transactions.
* **Receipt Printer**:
  + An integrated receipt printer is typically part of the ATM hardware to provide users with a physical record of their transactions.
* **Input Devices**:
  + Input devices such as a touch-sensitive display screen and a PIN pad are essential for user interaction. The display screen serves as the interface for users to navigate through transactions.
* **Network Interface**:
  + Hardware components for network connectivity, including network adapters or communication modules, are necessary for the ATM to connect to the banking network for transaction processing.
* **Secure Communication Protocols**:
  + Hardware support for secure communication protocols (e.g., SSL/TLS) ensures that data transmitted between the ATM and the banking network is encrypted and protected.
* **Internal Processing Unit**:
  + A powerful and secure processing unit (CPU) is essential for handling the computational demands of biometric authentication, transaction processing, and communication with the core banking system.
* **Memory (RAM and Storage**):
  + Adequate RAM is required for smooth operation, and sufficient storage (hard drive or solid-state drive) is needed for storing software, transaction logs, and system data.
* **Power Supply and Backup**:
  + A reliable power supply and backup system, such as an uninterruptible power supply (UPS), is critical to ensure continuous operation and prevent data loss in case of power outages.
* **Surveillance Cameras**:
  + Security cameras may be part of the hardware setup to monitor the ATM area and enhance security.
* **Environmental Controls**:
  + Climate control systems and environmental sensors may be necessary to ensure that the ATM hardware operates within specified temperature and humidity ranges.
* **Peripheral Components**:
  + Additional peripheral components may include barcode scanners, contactless card readers, or other devices depending on the specific features and functionalities of the ATM.
* **Anti-Skimming Devices**:
  + Anti-skimming devices may be incorporated into the hardware to prevent card skimming attempts.
* **Physical Security Features**:
  + Physical security features such as reinforced casings, tamper detection systems, and alarms enhance the overall security of the ATM hardware.

The hardware requirements for a fingerprint-based ATM system are diverse, and the specific components chosen will depend on the project's design, technical specifications, and security considerations. Collaborating with hardware vendors and ensuring compliance with industry standards is essential for a successful implementation.

**Pricing:**

Our fee for the whole project from the first step to the last one will be $[Total Fee Amount]. The breakdown is provided below:

|  |  |
| --- | --- |
| SOFTWARE DEVELOPMENT | Taka [ 20000000-50000000 (estimated)] |
| LAUNCH AND SUPPORT | Taka [7000000-20000000 (estimated)] |
| TRAINING | Take [2900000-6000000 (estimated)] |

**Warranty & Limitation of Liability**

The inclusion of warranty and limitation of liability clauses in the contract for a fingerprint-based ATM system project is essential to define the responsibilities of the parties involved and manage potential risks. These clauses outline the terms under which the system is provided, including assurances from the vendor (or developer) regarding the performance of the system and the extent of their liability in case of issues. Here is a general overview:

**Warranty:**

* **Limited Warranty Period:**
  + Specify the duration of the warranty period during which the vendor guarantees that the fingerprint-based ATM system will function as specified without defects.
* **System Performance:**
  + Clearly outline the expected performance standards and functionalities of the system during the warranty period.
* **Defects and Corrections:**
  + Define how the vendor will address and correct any defects or non-conformities identified during the warranty period. This may involve software updates, patches, or other corrective measures.
* **Exclusions from Warranty:**
  + Clearly state any exclusions from the warranty, such as issues arising from misuse, unauthorized modifications, or external factors beyond the vendor's control.
* **Hardware and Software Components:**
  + Specify the warranties associated with both hardware and software components, including any third-party components integrated into the system.
* **Limitation of Liability:**
* **Financial Limits:**
  + Clearly define the financial limits of the vendor's liability in the event of system failures, breaches, or other issues. This may include a cap on the total liability or a limitation on specific types of damage.
* **Indirect or Consequential Damages:**
  + Specify whether the vendor is liable for indirect or consequential damages, such as lost profits, business interruption, or reputational harm.
* **Force Majeure:**
  + Include a force majeure clause, stipulating that neither party is liable for failure to perform its obligations due to unforeseen circumstances beyond its control, such as natural disasters, acts of terrorism, or government actions.
* **Insurance:**
  + Specify any insurance requirements for both parties to mitigate potential liabilities.
* **Mitigation of Damages:**
  + Include a clause requiring both parties to take reasonable steps to mitigate damages in the event of a breach or failure.
* **Dispute Resolution:**
  + Outline the process for resolving disputes related to liabilities, such as mediation, arbitration, or litigation, and the associated costs.
* **Compliance with Laws:**
  + Ensure that the fingerprint-based ATM system and its operation comply with all applicable laws and regulations and clarify that the vendor is not liable for any issues arising from non-compliance by the client.
* **Client Responsibilities:**
  + Clearly outline the client's responsibilities, including the duty to follow proper security procedures, use the system as intended, and promptly report any issues.

It is crucial to involve legal professionals experienced in technology contracts to draft and review the warranty and limitation of liability clauses. The specific terms will depend on the unique circumstances of the project and the preferences of the parties involved. Additionally, the clarity and fairness of these clauses contribute to a positive and collaborative relationship between the vendor and the client.

**Contact us:**

You can contact us with any of the following ways:

Phone: [Contact Number]

E-mail: [E-mail Address]<mailto:XYZ@softwaresolutions.com>

Fax: [Fax Number]

Website: [website Address][http://www.xyzsoftwaresolutions.com/](http://www.XYZsoftwaresolutions.com)

We look forward to hearing from you.

Regards,

Web Dynamics