BIPO HRMS System Architecture

Introduction

BIPO HRMS is a cloud and mobile-based platform for Human Resources application, offering a suite of HRMS functions that significantly reduces manual work and optimize administrative workflow. This document describes BIPO HRMS system offering, architecture, and security.

BIPO HRMS Public Cloud SaaS Offering

BIPO HRMS is offered to customers in a SaaS (Software as a Service) model and using public cloud infrastructure, such as Amazon Web Services (AWS) and Alibaba cloud for its compute, storage and content processing. In this offering, customer data sits in a shared-server model, and each customer databases are logically segregated from each other.

Server Locations

AWS has 21 geographic regions around the world, while Alibaba cloud has 7 regions in mainland China, and 12 outside of China. Server location for a customer's BIPO HRMS instance is chosen based on AWS or Alibaba cloud region closest to the customer geographic location for the best performance.

As of Jan 2020, servers for BIPO HRMS instances are hosted in AWS Singapore and Hong Kong regions, and Alibaba Cloud Hong Kong and Shanghai regions. Servers in Singapore region serves BIPO customers in Singapore, Malaysia, Indonesia, Thailand, and Vietnam, while servers in Hong Kong and Shanghai serve BIPO customers in Hong Kong and mainland China. Servers in different regions can be deployed in future to meet new customer requirement.

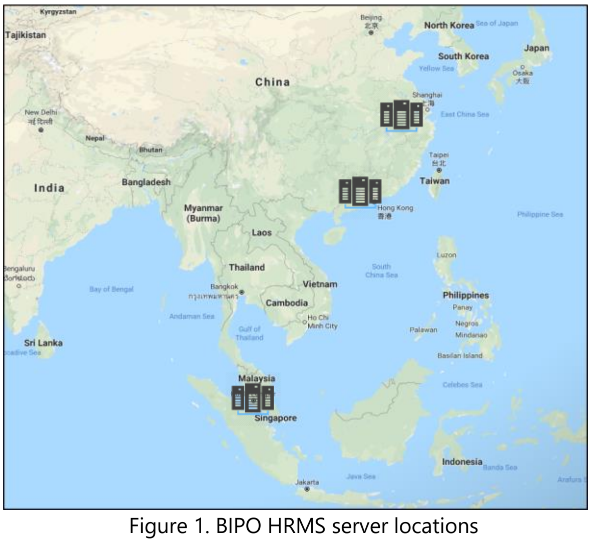


Figure 1. BIPO HRMS server locations

Other BIPO HRMS Offering

On-Premise

BIPO HRMS can be deployed on-premise within customer's data center for customers who want more control over their data. BIPO HRMS runs on Windows servers with IIS (for web server) and SQL Server (for database server). BIPO provides on-premise customers access to program update files for download on to their servers, released to all BIPO customers on monthly basis.

Private Cloud

Like on-premise installation, BIPO HRMS can be deployed on customer's private cloud, managed by the customer. Remote access is needed for BIPO IT to do software installation and system setup during project implementation. BIPO provides on-premise customers access to program update files for download on to their servers, released to all BIPO customers on monthly basis.

Logical View

BIPO HRMS users can be grouped into two: admin users and employees. Admin users perform HR functions and employee data processing, like setting leave and claims approval workflow, processing payroll calculation, generating pay slips, creating new employee record, etc. Employees use self-service functions to apply leave, apply claims, update personal particulars, apply for training, etc. Admin users use admin user module available in the web application. Employees use employee self-service (ESS) module available in both web and mobile application.

Web application can be accessed from popular Internet browsers on Windows and Mac OS. BIPO HRMS mobile app is available for IOS and Android devices. Below table summarize current supported browsers and platform for BIPO HRMS

	Supported Versions	**Remark**
Internet Browser	IE 11, Safari (latest), Chrome (latest), Edge	
Desktop OS	Windows 7, 10 (latest), Mac OS X (latest)	
Mobile App platform	Android 10, 9, 8, 7, 6, 5 (current and previous 5 versions) IOS 13, 12, 11, 10, 9 (current and previous 4 versions)	

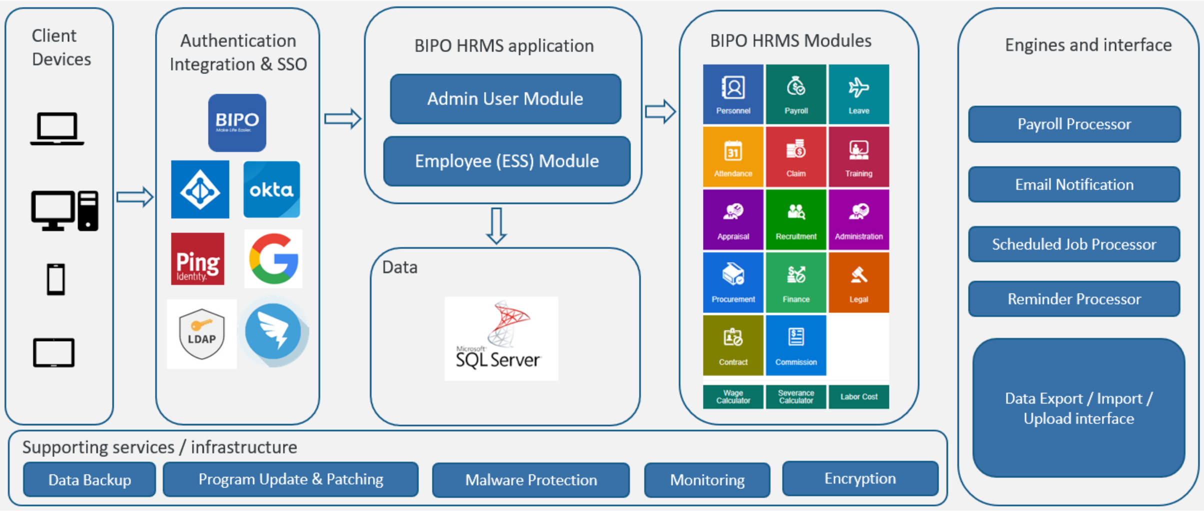


Figure 2. BIPO HRMS system components architecture

BIPO HRMS supports native authentication using local password for login. Password is stored in encrypted form using one-way hash function in BIPO HRMS database. BIPO also supports integration with other user directory service like LDAP, OKTA, Microsoft ADFS, Google Account, DingTalk, PING identity to delegate authentication to the third-party system and achieve Single Sign-On. BIPO supports integration using SAML 2.0 or OAuth protocol. User account is to be created from within BIPO HRMS. The mapping between the 2 user directories is established using the user email address, or login name, depending on the third-party user directory used.

User authorization is defined in BIPO HRMS, using menu access and user access settings. Menu access defines which menu items (pages, or page tabs) the user has access, and user access defines whether the kind of access the user has for each module (read only, or read-write), and the employee groups that the user has access to (e.g. employees of specific department only).

User access to BIPO HRMS via the Internet is secured by encryption using TLS (Transport Layer Security). This protects traffic from eavesdropping and tampering of messages. Traffic from application server to database is also secured via encrypted connection for SQL Server instance. BIPO provides secure FTP connection for customer to upload data for data import. Option for data at rest AES 256 encryption using SQL Server Transparent Data Encryption (TDE) is available as well.

Customer database is backed up every 4 hours and stored in separate cloud storage that is replicated across multiple data center locations (availability zones) in the same region. System is continuously monitored for any issues (e.g. server resource utilization issue, failed scheduled jobs, backup job status) to alert person in charge in BIPO for immediate action. All BIPO HRMS servers are protected with anti-malware software auto-updated virus signature, patched regularly with OS security patches and BIPO HRMS program updates.

BIPO HRMS supports different payroll calculations for different countries, the payroll engine is in-house developed by BIPO RND team whenever a new country is added into the list of supported countries. Email notification system sends notifications such as leave pending approval, request application approval status, as well as scheduled job exceptions. Scheduler program is responsible for running scheduled jobs at predefined schedule, and reminder program sends reminder emails to requestor when there are pending request not submitted yet, or to approver when there are requests pending for approval.

BIPO HRMS comes with data export functions to export master tables (e.g. company, department, cost center, pay group, leave grade, etc.) to csv format files. Import or upload functions provides the means for admin users to upload csv data files from server (import) or from their PC (upload) into the master tables. Import job can also be scheduled for example, to import attendance data from customer's on-premise clocking system into BIPO HRMS. The attendance data is uploaded from customer's on-premise system to the HRMS server via SSH FTP (SFTP) interface.

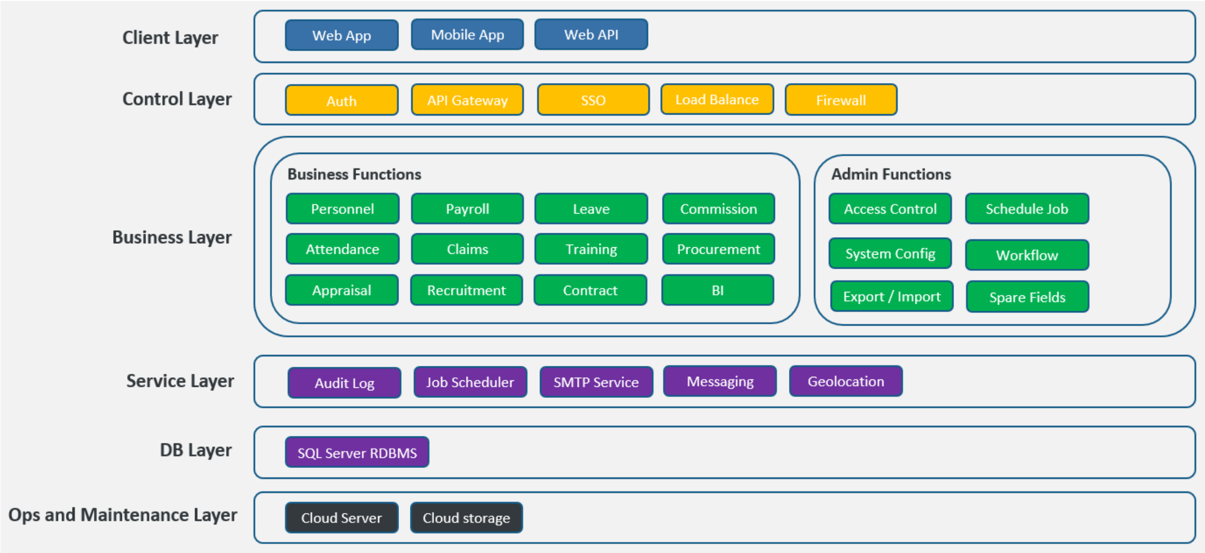


Figure 3. BIPO HRMS layered architecture

BIPO HRMS applications is available as web application (admin and employee self-service modules), accessible from Internet browser. It is also available as mobile application (employee self-service module), accessible from BIPO HRMS mobile app.

BIPO HRMS provides Web API to external system for data exchange via web API call. Web API user credentials and access method are maintained in HRMS system and each user can be assigned certain API functions. Each web API call will include access token with expiry, generated using OAuth2 tokenizer. Once access token expires, it can be generated again using the tokenizer, using the corresponding web API user credential for the external system.

For native authentication, user password can be governed using password policy settings that can be set according to each customer requirement (e.g. minimum password length, password complexity requirement, account lock period, etc.). Authentication can be delegated to third-party user directory like Microsoft ADFS or Google account to achieve Single Sign-On. BIPO HRMS support SAML 2.0 and OAuth2 protocol for this integration.

For HRMS system with HA setup, load balancer is used to distribute the workload across multiple nodes to scale out in compute power as well as providing node redundancy.

Access to BIPO HRMS application is secured using web application firewall and network firewall. Cloudflare web application firewall inspects web request traffic and challenge or block malicious one and forward valid traffic to the web server. Network firewall restricts access to the server based on source IP address and network port and protocol.

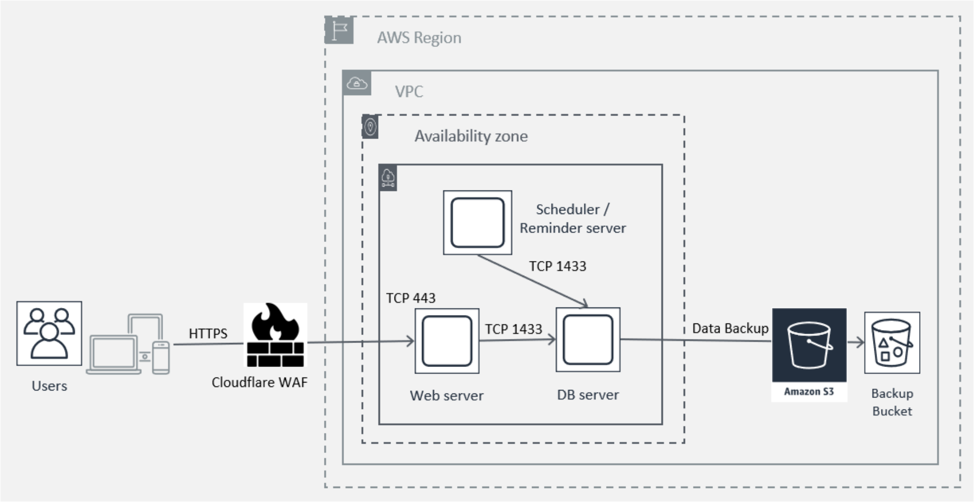
BIPO HRMS application has several business modules. Based on customer license agreement, the corresponding business modules will be enabled for the customer's HRMS instance. Admin functions are available across all business modules, providing admin users to provide the right access to each user, set system settings, perform data export / import functions, schedule batch jobs, change approval workflow rules, and make use of spare fields to capture additional information outside of the predefined fields if needed.

Audit log in HRMS system includes activity log and data log. Activity log captures user activity such as login/logoff events (including failed login attempts) and menu items (page or page tab) accessed by the user. Data log captures data changes before and after the change.

Messaging service provides notification in mobile app for things that require the user attention, e.g. pending tasks. Geolocation service is used in Attendance module in mobile application. Employees can perform clocking using the HRMS mobile app and the system will verify the user's geolocation against approved clocking location in the process.

Physical View

The diagram below describes BIPO HRMS network architecture. HRMS servers run in public cloud infrastructure from Amazon AWS or Alibaba Cloud. For standard HRMS setup, both web server and database server are in the same data center location (availability zone).



Software to Hardware Mapping

The below table indicates where the various BIPO HRMS software components are deployed

Software component	Client	Web Server	DB Server	Scheduler / Reminder Server	Remark
Internet browser	✓				
Mobile app	✓				
IIS web server		✓			
SQL Server			✓		
HRMS app binaries		✓			
HRMS db programs			✓		Programs stored inside HRMS database
Scheduler / Reminder programs				✓	May be installed on web server
SFTP server		✓			For upload of interface csv files from customer system
AWS CLI		✓	✓		Used to upload backup files to Cloud storage

Communication Flow

The below table details how communications will flow between different components of the solution

Flow	Nodes	Protocol	Port	Comments
1	Client, web server	HTTPS	443	For access to HRMS application from web browser or mobile ap
2	Web server, db server	TCP	1433	For access to HRMS database from web server
3	Scheduler/reminder server, db server	TCP	1433	For access to HRMS database from scheduler / reminder server

4	Web server, AWS S3	HTTPS	443	For backup of attachment files to S3
5	DB server, AWS S3	HTTPS	443	For backup of database to S3

Monitoring

Monitoring tools for BIPO HRMS instance include AWS Cloudwatch, AWS SNS, AWS SES, AWS CloudTrail, BIPO HRMS email notification, and custom scripts managed by BIPO IT Administrators. IT administrators and person in charge are alerted for issues that need attention (e.g. server resources issues, changes to firewall rules, instance up / down status, schedule job exceptions, backup job statuses).

Backup / Restore

Backups of HRMS instance are stored in S3 cloud storage, with replication across multiple data center locations (availability zones) in the same region. HRMS database is backed up every 4 hours and test restore is performed periodically to verify validity of the backup media.

Patching

Windows updates are applied to all BIPO HRMS servers regularly by BIPO IT team. HRMS program updates are released every 2 weeks and applied to all HRMS SaaS instances every 4 weeks after they are tested internally by BIPO QA team.

High Availability

BIPO HRMS severs run on Amazon AWS and Alibaba cloud infrastructure. These cloud providers are ISO 27001 certified and their data centers are equipped with redundant facilities and hardware (power, network, cooling, humidity control, disk storage, servers) to tolerate any failure without impact to customer’s running instances.

BIPO HRMS standard instance runs on single web and database servers. Special server setup can be made for customers that need high availability for their HRMS instance, where multiple web servers run behind load balancer and the database runs in a SQL Server cluster.

Disaster Recovery

Both AWS and Alibaba Cloud block storage is designed with high durability and availability allowing hardware part failure to be replaced without downtime to customer instances. Should and availability zone where BIPO HRMS production instance runs become unavailable, the affected production instance will be restored in another availability zone in the same region, using most recent disk snapshot and database backup. Snapshots and database backups are replicated across multiple availability zones in AWS and Alibaba cloud infrastructure. The SLA for the BIPO Production Service disaster recovery is a 24-hour recovery time objective (RTO) and a 4-hour recovery point objective (RPO).

Security View

Infrastructure Security Control

To maintain network and application security vulnerability assessment and penetration testing are conducted on BIPO HRMS application on regular basis to identify and address new vulnerabilities. Assessment is done by independent third-party IT security vendor.

BIPO HRMS web application is protected with third-party web application firewall protecting the web site from web application vulnerabilities. Identified new threats are automatically added into the web firewall database, providing always-up-to-date protection.

BIPO HRMS servers are patched against new vulnerabilities regularly with patches from Microsoft for Windows Servers and SQL Servers.

Application Security Control

All user activity inside the application are logged in application activity log and data log. Activity log captures actions perform within the application and data log captures information before and after change. All users are IT Administrator use individual login IDs with their activity logged for auditing and accountability.

BIPO HRMS security access is menu-based, assigned to users based on their role. Read-only or read-write access can be set for each function, and user activity and changes in the application are logged inside application and data log all the time.

BIPO HRMS supports SAML for integration with customer’s single-sign-on (SSO), and with Microsoft and Google account authentication.

BIPO HRMS native login uses application account password governed by many password policy settings that can be adjusted to meet customer’s password policy requirement (minimum length, complexity, expiry, account lock out, etc.). Login attempts, both successful and unsuccessful, are logged for audit purposes. Inactive user sessions are automatically timed out after a specified time configured according to customer requirement.

Data Security Control

BIPO HRMS is a multi-tenant SaaS application. Multiple customers share one physical instance of BIPO HRMS system with each customer tenant's application data isolated from each other.

Each customer web application is linked to only one client ID which restricts the client database it can connect to.

User access to BIPO HRMS via the Internet is secured by encryption using TLS (Transport Layer Security). This protects traffic from eavesdropping and tampering of messages. Traffic from application server to database is also secured via encrypted connection for SQL Server instance. BIPO provides secure FTP connection for customer to upload data for data import. Option for data at rest encryption using SQL Server Transparent Data Encryption (TDE) is available.