WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:

receiving, by a polling service system, a first Application Programming Interface (API) request from one or more source devices through a first endpoint, wherein the first API request indicates requirement of the one or more source devices to perform one or more data transactions with a corresponding candidate application server;

parsing, by the polling service system, the first API request of each of the one or more source devices to identify the requirement of the one or more source devices;

generating, by the polling service system, a unique first response for each of the one or more source devices based on the requirement corresponding to the one or more source devices, wherein the unique first response generated for each of the one or more source devices comprises a unique second endpoint that facilitates the one or more data transactions with the corresponding candidate application server; and

transmitting, by the polling service system, the unique first response generated for each of the corresponding one or more source devices, wherein each of the one or more source devices use the corresponding unique second endpoint to perform the one or more data transactions with the corresponding candidate application server;

wherein the unique first response further comprises at least one of the following: parameters required for performing the one or more data transactions with the corresponding candidate application server and a unique transaction token for validation purposes, an encryption key, one or more input fields for an API call, or any combination thereof; and

wherein the unique second endpoint is dynamically generated in response to each of the first API requests based on one or more predefined rules, wherein the one or more predefined rules are related to at least one of the following: a version of a corresponding candidate application facilitating the corresponding candidate application server, criticality of the requirement of the one or more source devices, geographic location of the one or more source devices, validity time of the unique second endpoint, or any combination thereof.

2. The computer-implemented method of claim 1, wherein the one or more source devices are validated prior to generation of the unique first response.

3. The computer-implemented method of claim 1, further comprising storing, by the polling service system, intimation information corresponding to each of the generated unique first responses, wherein the intimation information comprises a unique transaction token provided to the one or more source devices for validation purposes, and at least one of the following: an identifier of the one or more source devices, details of the unique second endpoint to be provided to the one or more source devices, an identifier of the corresponding candidate application server that the one or more source devices are allowed to access through the unique second endpoint, or any combination thereof.

4. The computer-implemented method of claim 1, wherein the first API request comprises at least one of the following: a device Identifier (ID) of the one or more source devices, an Internet Protocol (IP) address associated with the one or more source devices, latitude and longitude associated with the IP address, a device score, a device type, an initial base token, a product ID, action code, user ID, pre-address ID, metadata required to complete the one or more data transactions, or any combination thereof.

5. The computer-implemented method of claim 1, further comprising:

receiving, by the corresponding candidate application server, a second API request from the one or more source devices through the corresponding unique second endpoint, wherein the second API request comprises parameters and metadata required for performing the one or more data transactions with the corresponding candidate application server;

validating, by the corresponding candidate application server:

if the one or more source devices are trusted sources, and

if the second API request received through the corresponding unique second endpoint is a valid request; and

transmitting, by the corresponding candidate application server, upon successful validation, a second response to the one or more source devices, through the corresponding unique second endpoint, wherein the second response is generated upon performing the one or more data transactions comprising at least one of the following: data retrieval, modification of data elements, addition of data elements, deletion of data elements, replacement of data elements, or any combination thereof, and wherein the second response comprises at least one of acknowledgement related to the one or more data transactions and data related to the one or more data transactions.

6. The computer-implemented method of claim 5, wherein the validating comprises:

retrieving, by the corresponding candidate application server, intimation information related to the corresponding candidate application server from a polling database associated with the polling service system; and

comparing, by the corresponding candidate application server, the intimation information with a corresponding unique transaction token present in the second API request of the one or more source devices to determine a match.

7. The computer-implemented method of claim 6, further comprising performing one of accepting or rejecting, by the corresponding candidate application server, the second API request, if the comparison determines the match or a mismatch, respectively.

8. A polling service system comprising:

a processor; and

a memory communicatively coupled to the processor, wherein the memory stores processor instructions, which, on execution, causes the processor to:

receive a first Application Programming Interface (API) request from one or more source devices through a first endpoint, wherein the first API request indicates requirement of the one or more source devices to perform one or more data transactions with a corresponding candidate application server;

parse the first API request of each of the one or more source devices to identify the requirement of the one or more source devices;

generate a unique first response for each of the one or more source devices based on the requirement corresponding to the one or more source devices, wherein the unique first response generated for each of the one or more source devices comprises a unique second endpoint that facilitates the one or more data transactions with the corresponding candidate application server; and

transmit the unique first response generated for each of the corresponding one or more source devices, wherein each of the one or more source devices use the corresponding unique second endpoint to perform the one or more data transactions with the corresponding candidate application server;

wherein the unique first response further comprises at least one of the following: parameters required for performing the one or more data transactions with the corresponding candidate application server and a unique transaction token for validation purposes, an encryption key, one or more input fields for an API call, or any combination thereof; and

wherein the unique second endpoint is dynamically generated in response to each of the first API requests based on one or more predefined rules, wherein the one or more predefined rules are related to at least one of the following: a version of a corresponding candidate application facilitating the corresponding candidate application server, criticality of the requirement of the one or more source devices, geographic location of the one or more source devices, validity time of the unique second endpoint, or any combination thereof.

9. The polling service system of claim 8, wherein the one or more source devices are validated prior to generation of the unique first response.

10. The polling service system of claim 8, wherein the processor is further configured to store intimation information corresponding to each of the generated unique first responses, wherein the intimation information comprises a unique transaction token provided to the one or more source devices for validation purposes, and at least

one of the following: an identifier of the one or more source devices, details of the unique second endpoint to be provided to the one or more source devices, an identifier of the corresponding candidate application server that the one or more source devices are allowed to access through the unique second endpoint, or any combination thereof.

11. The polling service system of claim 8, wherein the processor generates the unique second endpoint dynamically in response to each of the first API requests based on one or more predefined rules, wherein the one or more predefined rules are related to at least one of the following: a version of a corresponding candidate application facilitating the corresponding candidate application server, criticality of the requirement of the one or more source devices, geographic location of the one or more source devices, validity time of the unique second endpoint, or any combination thereof.

12. The polling service system of claim 8, wherein the first API request comprises at least one of the following: a device Identifier (ID) of the one or more source devices, an Internet Protocol (IP) address associated with the one or more source devices, latitude and longitude associated with the IP address, a device score, a device type, an initial base token, a product ID, action code, user ID, pre-address ID, metadata required to complete the one or more data transactions, or any combination thereof.

13. The polling service system of claim 8, wherein the corresponding candidate application server associated with the polling service system is configured to:

receive a second API request from the one or more source devices through the corresponding unique second endpoint, wherein the second API request comprises parameters and metadata required for performing the one or more data transactions with the corresponding candidate application server;

validate:

if the one or more source devices are trusted sources, and

if the second API request received through the corresponding unique second endpoint is a valid request; and

transmit, upon successful validation, a second response to the one or more source devices, through the corresponding unique second endpoint, wherein the second response is generated upon performing the one or more data transactions comprising at least one of the following: data retrieval, modification of data elements, addition of data elements, deletion of data elements, replacement of data elements, or any combination thereof, and wherein the second response comprises at least one of acknowledgement related to the one or more data transactions and data related to the one or more data transactions.

14. The polling service system of claim 13, wherein, to validate, the corresponding candidate application server is configured to:

retrieve intimation information related to the corresponding candidate application server from a polling database associated with the polling service system; and

compare the intimation information with a corresponding unique transaction token present in the second API request of the one or more source devices to determine a match.

15. The polling service system of claim 14, wherein the corresponding candidate application server performs one of accepting or rejecting the second API request if the comparison determines the match or a mismatch, respectively.

16. A non-transitory computer-readable medium including instructions stored thereon that when processed by at least one processor, causes a polling service system to perform operations comprising:

receiving a first Application Programming Interface (API) request from one or more source devices through a first endpoint, wherein the first API request indicates requirement of the one or more source devices to perform one or more data transactions with a corresponding candidate application server;

parsing the first API request of each of the one or more source devices to identify the requirement of the one or more source devices;

generating a unique first response for each of the one or more source devices based on the requirement corresponding to the one or more source devices, wherein the unique first response generated for each of the one or more source devices comprises a unique second endpoint that facilitates the one or more data transactions with the corresponding candidate application server; and

transmitting the unique first response generated for each of the corresponding one or more source devices, wherein each of the one or more source devices use the corresponding unique second endpoint to perform the one or more data transactions with the corresponding candidate application server;

wherein the unique first response further comprises at least one of the following: parameters required for performing the one or more data transactions with the corresponding candidate application server and a unique transaction token for validation purposes, an encryption key, one or more input fields for an API call, or any combination thereof; and

wherein the unique second endpoint is dynamically generated in response to each of the first API requests based on one or more predefined rules, wherein the one or more predefined rules are related to at least one of the following: a version of a corresponding candidate application facilitating the corresponding candidate application server, criticality of the requirement of the one or more source devices, geographic location of the one or more source devices, validity time of the unique second endpoint, or any combination thereof.

17. The medium of claim 16, wherein the instructions cause the corresponding candidate application server associated with the polling service system to:

receive a second API request from the one or more source devices through the corresponding unique second endpoint, wherein the second API request comprises parameters and metadata required for performing the one or more data transactions with the corresponding candidate application server;

validate:

if the one or more source devices are trusted sources, and

if the second API request received through the corresponding unique second endpoint is a valid request; and

transmit, upon successful validation, a second response to the one or more source devices through the corresponding unique second endpoint, wherein the second response is generated upon performing the one or more data transactions comprising at least one of the following: data retrieval, modification of data elements, addition of data elements, deletion of data elements, replacement of data elements, or any combination thereof.