Open-Automated Teller Machines for Dynamic Transactions and Data Access

A. A. Periola,[1*], A. A Alonge[2], K. A. Ogudo[3]

[1]Department of Electrical, Electronic and Computer Engineering, Faculty of Engineering and the Built Environment, Cape Peninsula University of Technology, Cape Town, South Africa.

[2]Department of Computer Systems Engineering, Faculty of Engineering and the Built Environment, Tshwane University of Technology, Pretoria, South Africa.

[3]Department of Electrical, and Electronic Engineering Technology, Faculty Engineering and Built Environment, University of Johannesburg, Johannesburg, South Africa.

ABSTRACT: The Automated Teller machine (ATM) is the workhorse of modern financial service delivery to end–users. The ATM is owned and deployed by a given financial service provider or bank. The bank's account holders can access financial service providers via their ATM card. Individuals who operate accounts with other financial service providers can also use the ATM belonging to another financial service provider. However, this incurs an additional service charge. Individuals seek to execute more transactions on an ATM besides cash withdrawals. Some of these transactions are specific to a financial service provider and cannot be executed on the ATM of other financial service providers. This is challenging because financial service providers do not conduct significant cross–functional collaboration in ATM design and deployment. The discussion in this paper seeks to address this challenge and proposes the open–automated teller machine (O–ATM). The O–ATM incorporates software and hardware payload realized by the co–hosting of multiple financial services from different financial service providers. The discussion presents the proposed O–ATM, its entities and describes how the entities function and relate with each other. The role of the O–ATM in enhancing the access to data storage via cloud computing is also recognized. In addition, performance analysis shows that the use of the O-ATM enhances the ATM deployment density and cloud service reach by an average of 21.2%, and 63%, respectively.

KEYWORDS: Automated Teller Machines, Network Integration, Cloud Computing, Data Access Systems

[Received July. 7, 2025; Revised June 13, 2025; Accepted Jun 28, 2026] Print ISSN: 0189-9546 | Online ISSN: 2437-2110

I. INTRODUCTION

The automated teller machine (ATM) plays an important role in the delivery of financial services in the 21st century society. An ATM constitutes an important component in the workhorse of a modern bank. It enables the execution of actions related to cash deposits, cash withdrawals, inter–bank account transfers and payment of utility bills. The ATM benefits from advances in artificial intelligence, networking, computing operating systems, information storage, database, and security. Currently, banks each deploy their ATM separately for access to individuals at different locations (Velayuthapandian et al., 2024, Carbo-Valverde et al., 2014, Ciaccio et al., 2025). The ATMs are accessed by different types of individuals who own an access card (called the ATM card) for each bank (Mubiru et al., 2024, Suder et al., 2022). In the case where the individual does not have an account with the financial services provider owning the ATM, the individual is levied an additional operational and access charge.

However, significant challenges arise with the use of the ATM in modern society. Some of these challenges are (1) Inflexibility associated with accessing cash via the ATM, (2) Long wait times at ATM queues, (3) inflexibility of user menu, and (4) inability of an individual to gain a-priori awareness of ATM functional status. These challenges are interconnected. For example, a long ATM wait time can arise when the user with account in one financial services provider aims to use the ATM (with a different display interface) of another financial services provider; the resulting delay arises because of the time taken to adjust to using the interface menu in the ATM of another financial services provider. Such a challenge can arise due to cognitive decline in the intending ATM user.

In addition, there is an inflexibility associated with accessing cash through deployed ATMs. This challenge arises because ATMs are sited in fixed terrestrial locations requiring intending users to pay a physical visit. However, innovative solutions have been proposed to address this challenge. The use of unmanned aerial vehicles has a significant potential in the realization of highly mobile ATMs. The use of drones is appealing because of their high mobility which is achievable at low costs. However, the use of drone ATMs is challenging due to the global governmental restrictions on unmanned aerial vehicle usage in different applications. Such restrictions apply in Africa too (Ayamga et al., 2021, Akinradewo et al. 2024, Daoud et al., 2025).

*Corresponding author: periola@hotmail.com

doi: http://dx.doi.org/10.63746/njtd.v23i2.3804

The emergence of cloud computing has been recognized to be capable of transforming ATM installation. The configuration of multiple ATMs via the cloud is recognized to be efficient in comparison to a manual configuration via individual visits (Rana et al., 2023, Greene, 2018, SBS, 2023). Technologies such as facial recognition can also enhance the security of individuals utilizing the ATM for financial transactions (Patil et al., 2024).

Another challenge that increases individual wait duration is menu inflexibility across ATMs deployed by different and multiple financial services providers. This is because financial service providers have unique services that are customised and designed only for access via their own custom design ATMs. The challenge arises because financial service providers do not collaborate on ATM interface menus design. This results in individuals not being able to access certain services when ATMs from certain financial service providers in a geographical region are non-functional. A solution to this challenge is the design of multi–service provider, multi–contextual multi-lingual, and intelligent ATM.

The modern ATM is ubiquitous and accessible to a significant number of users. ATMs also incorporate networking capability and benefit from advances in information and communication technologies. This makes it feasible to consider the ATM as a cloud access node in communication networks. In its role as cloud access node, the ATM executes activities such as data upload and download. ATM functioning in this capacity requires a constructive interaction between financial service providers, mobile wireless networks, and cloud computing providers. This has not received sufficient consideration in wireless networking research. This paper proposes a multi-mode open ATM (O–ATM) with the capability to execute financial services and access cloud computing platforms. The O–ATM modes are finance and cloud modes.

The proposed research presents the functional and entity architecture of the O-ATM discussing the role of its entities, executed processes and inter-entity relations associated with the O-ATM. The O-ATM has the benefits of enhancing the conduct of customer oriented financial transactions. The use of the O-ATM reduces the number of ATMs that are deployed by financial service providers in reaching the client and customer base. It reduces ATM under-utilization epoch. The rest of the discussion is structured as follows. Section II discusses the background work. Section III addresses the challenges arising from the current ATM model. It also proposes the new ATM model and describes how its functionalities affect the functionality of the proposed ATM model. Section IV describes how the future ATM can address the challenge associated with the access to cloud computing access at a retail level. Section V focuses on the performance analysis. Section VI is the conclusion.

II. DISCUSSION OF BACKGROUND WORK

The discussion in (Rahaman et al., 2025) recognizes that the reliance on the personal identification number for automated teller machine poses a single point of attack and constitutes a security risk. The research proposes the use of a cardless approach of using automated teller machine. The use of the cardless approach removes the personal identification number from the automated teller machine (ATM) access dynamics. The approach being proposed is the block-chain driven single sovereign identity. The single sovereign driven identity presents a solution that shifts the ATM security away from the financial organization. In this case, the use of the smartphone is proposed for ATM financial service access. The reliance on the smartphone introduces new challenges from resulting dynamics. An important challenge to be addressed is that the ATM security is now influenced by increasing smartphone theft.

An internet of thing (IoT) based security-based mechanism is proposed for ATM in the discussion in (Nafis et al., 2025). The proposed mechanism uses integrated blockchain technology incorporated with IoT edge nodes for the security using the RSA and AES encryption standards. Essentially, the research proposes using a distributed ledger technology for transaction verification via the use of low-latency fog-based computing system. The use of the proposed approach relies on the availability of extensive distributed fog nodes associated with computing networks. The coordination of the multiple fog nodes by the multiple anchoring communication networks requires the design of a supporting communication network. Furthermore, a challenge that should be addressed is power availability for a significant number of fog nodes. This is especially important for the case of regions having challenges with power security.

Sergiv et al., (2025) propose the use of video via digital devices for improving user authentication security while executing financial transactions on ATMs. The discussion in [20] recognize that the misuse of certain ATM parts such as ATM cash acceptor bays pose an initial step for later malicious ATM user attack via the insertion of harmful objects. The focus and core of the proposed solution is that of analysing the emotional state of the ATM user. The emotional state's associated data is received via video from the ATM. In this case, the ATM hosts a camera and a convolutional neural network for executing image-linked associated emotional state analysis. The image-linked associated emotional state analysis is done using streaming video. This requires the availability of camera functionality at the ATM. The occurrence of camera unreliability or detection of camera location affects the suitability of the proposed solution.

Garcia (2025) propose the use of a fingerprint as a unique user bio-signature for realizing ATM security. In the proposed approach, the fingerprint scanner is integrated into the ATM. The proposed approach uses a biometric engine that validates the fingerprint input against a database. The use of an integrated fingerprint approach has the benefits of having a low latency between obtaining the user focused bio-signature for analysis. The challenge associated with the proposed approach in (Garcia, 2025) is that the quality of the finger-print scanner influences the performance of the fingerprint scanning based ATM security approach. Additional research is required to evaluate the performance of different fingerprint scanners and the suitability for financial ATM integration.

Paul (2025) recognizes the need to integrate the financial ecosystem with the fifth-generation internet of thing (5GioT) context. This is recognized to be essential from the perspective

of increasing the public awareness of the 5G technology and its usefulness in the financial technology domain. The discussion essentially provides a survey that is forward looking by proposing the integration of the 5G technology. This integration provides a base for the emergence of new application contexts. However, a consideration in this direction requires further research.

III. FIRST ASPECT: - OPEN ATM MODEL FOR FUTURE FINANCIAL TRANSACTIONS

The discussion in this section presents the proposed O-ATM and how it enhances future financial transaction. The rest of the discussion is structured as follows. Section A describes the problem being addressed. Section B presents the architecture of the proposed open ATM.

A. Problem Description

The problem being addressed considers a scenario with multiple financial service providers. Each financial service providers deploys ATMs over a wide geographical area. Each financial services provider has ATMs with a pre–designed and pre–configured interface that hosts pre–specified combination of menus and submenus. The menu describes the list of activities supported by the financial services provider or services that are delivered to the subscriber(s). The ATMs of financial service providers can lie within a geographical range in clusters that can be approached by the individual seeking to execute a financial transaction on the ATM. Financial service access challenges to individuals arise in the following scenarios:

Scenario 1: The individual seeks to utilize ATM of own bank to execute actions related to making a transfer to a deposit interest earning account. The ATM of the concerned individual's financial service provider is non-functional. However, the ATM of another bank within the same geographical region is functional. The individual is unable to make the desired deposit and associated transfer because the menu and interface of the active ATM does not support the execution of the desired transaction.

Scenario 2: An individual seeks to check the current balance in an investment account. The investment account has been opened with a financial services provider with deployed and operational ATMs. However, the deployed and operational ATMs for the financial services provider domiciling the investment account is not functional at the concerned location. This makes it challenging for the individual to check the desired balances in the account.

Scenario 3: The individual seeks to execute financial transaction at a given geographical region. The location has multiple ATMs from different financial service providers available. However, each ATM has different queue lengths i.e. varying number of individuals desiring to use the ATM to execute their financial transactions. In the case being considered, the ATM with the shortest queue (expected waiting time) for the individual is not that belonging to the financial services provider where the investment account is domiciled. Nevertheless, it is important that the concerned individual be able to execute all the financial transactions that are desired.

Scenario 4: The individual desires to execute an ATM driven cash deposit. In this case, the individual has an account that is operational with a given financial services provider. However, the concerned financial services provider does not have a functional ATM at the location of the concerned individual. In addition, the individual is at a location which is significantly distant from the nearest ATM owned by the financial service provider where the account is initially domiciled. The individual should be able to make the concerned cash deposit via the available, accessible, and functional ATM (belonging to another financial service provider) at the individual's current location.

Scenario 5: The individual seeks to execute a financial transaction involving a cash deposit via the ATM. The individual's location has multiple ATMs belonging to different financial service providers. In this case, the available ATMs have different technological capabilities. Some ATMs have cash deposit capabilities while others do not have cash deposit capabilities. The ATM belonging to the financial services provider providing banking services to the concerned individual does not have a cash accepting capability. However, it is important that the individual be able to execute the required cash deposit transaction. This is deemed necessary for security motives.

Scenario 6: The case being considered here is an extension of scenario 5. In this case, there are multiple ATMs belonging to different financial service providers at the individual's location. However, each ATM has a limited capacity on the amount of cash that can be accepted from an individual with an account domiciled with another financial service provider. In this case, it is necessary that the individual be able to utilize ATMs (with cash accepting capabilities) from different financial service providers.

Scenario 7: The individual seeks to execute cash deposit or investment account deposit into different accounts. The concerned accounts are domiciled with different financial service providers. In this case, the financial service providers involved in the financial transaction does not have functional ATMs in the location of the concerned individual. In this case, it is important that the individual be able to execute the transactions on the ATM of another financial service provider at the current location.

Scenario 8: An individual seeks to execute a financial transaction exclusive of cash withdrawal at a given location. In this case, the ATM belonging to a financial service provider (with which the individual has the account) is not available or non-functional. Furthermore, the ATM of another financial service provider that is available at the individual's location is unable to support the execution of the individual's desired transaction. However, the available ATM is reconfigurable.

The challenges in Scenarios 1–8 arise because of the proprietary nature of the ATM interface. The proprietary nature arises because each financial service provider has own software and hardware development team. Each development team conducts research separately towards the design of proprietary interface for the concerned financial services provider. However, the design of an open–ATM can address these challenges. An O-ATM can make possibilities available to individuals in the delivery of financial services.

B. Proposed Solution: Open–Automated Teller Machine

This section describes the proposed open–automated teller machine (O–ATM). The O–ATM enables multiple financial service providers to bundle their services together and realize a unified service delivery. Though the considered context is that of traditional and government recognized and licensed financial institutions, it is important that the O–ATM accommodates non–traditional financial service providers. The O–ATM is realized via an open–funded and open–acquisition strategy involving multiple financial service providers. In realizing the O–ATM, hardware and software development teams from financial service providers work collaboratively. Each financial service provider incorporates the following software components in the O–ATM:

Financial Services Scripts: The financial services script (FSSs) describes the graphical user interface (GUI). The GUI presents the interface enabling the individual to select the desired transaction. The FSS also comprises the code for the implementation of the financial transaction that is associated with all menus and submenus. The menus and the submenus are those associated with options for financial services being offered to the individual. The GUI is designed to have menus that support the user to select multiple languages and different service menu options. This is in line with the design of user interfaces for emerging financial technologies and solutions (Runsewe et al., 2024, Ali, 2025).

Network Access Scripts and Commands (NASCs): The NASCs describes the instructions enabling access to the database of the financial service provider. The database holds the information on the record of the individuals with accounts domiciled with the financial service provider. The FSS and NASC software entities are defined by the software development team of the financial service provider. The O–ATM also incorporates hardware components. The hardware components provide the computational resources and capabilities enabling the realization of the functionality of the proposed FSSs and NASCs software components. The financial service provider's hardware development team provides the specification of the hardware components. The hardware components enable communications and computing in the O–ATM. The communications payload comprises a router with software defined radio (SDR). The SDR enables the router to reconfigure its operational parameters for data communications with specifications in the NASC. SDR re–configuration is prompted by the individual's choice of a given financial service provider while using the O–ATM. The router communicates with the back–end database of the financial service provider via a mobile wireless network.

The computing payload is realized using neuromorphic hardware that hosts the financial service provider's FSS. The use of neuromorphic computing hardware is considered due to the low power consumption and inherent support for artificial intelligence based financial service solutions. The neuromorphic hardware aboard the O–ATM provides the computing resources required to execute the FSSs provided by each financial service provider. The FSSs hosts additional information besides the GUI that is associated with the financial services accessed by an individual. In this case, the utilized neuromorphic hardware is adapted from the existing offerings available from original equipment manufacturer such as IBM True North. In this case, IBM True North hardware is recognized because of its support for functional re-programmability (Xu et al., 2025) relating to the FSS for each financial service provider. In the use of the proposed O-ATM, a user initially selects their own financial institutions from a page menu.

This selection is the input that triggers the O-ATM FSS process and mode switching for loading the menu corresponding to the selected financial institution by the user. This is feasible considering that electronic switching can be realized in the time range 40seconds–45 seconds for the application specific integrated circuit used in the IBM True North neuromorphic system. In the case of the proposed O-ATM, a system level reconfiguration and not a chip-level reconfiguration is executed. Therefore, the switching latency is less than a minute and does not constitute significant latency to the O-ATM services. In addition, the O–ATM incorporates a visual display subsystem (VDS) that comprises all entities and components enabling the display of menu, submenus, and transaction options to the individual. The VDS functionality depends on the O-ATM's ownership model. The O–a single financial service provider can own ATM. The financial service provider's menu and sub–menu interface influences menu key functionalities on the O–ATM.

Another plausible scenario is one in which the O–multiple financial services providers own ATM. In this case, a clickable screen menu is utilized. The choice of a menu that is clickable via the screen in the VDS is considered for ease of use by the considered individual. The O–multiple financial service providers can also own ATM. In this case, other financial service provider brings the communications and computing payload into the O–ATM. The O-ATM's functionality is described in this section. The relations between the FSSs, NASCs the computing payload and communications payload is shown in Figure 1. From the relations in Figure 1, the user interacts directly with the VDS (clickable screen, menu, and submenu). The VDS engages in a bi–directional relation with the computing payload. The computing payload has bi–directional relations with the communications payload. The SDR aboard the communications payload connects to the database of the financial service providers. This connection (not shown) is realized wirelessly via ubiquitous mobile wireless networks. In the O–ATM, application programming interfaces (APIs) enable the neuromorphic computing payload, communication payload, and the clickable screen to communicate with each other.

The neuromorphic computing payload provides computational resources enabling the execution of integrating APIs. The neuromorphic computing payload coordinates communications with the communication payload and the graphic user interface (GUI) i.e., the clickable screen. The APIs in the neuromorphic computing payload enables the communication with logical interfaces in the communication payload and the GUI. Each of the logical interfaces hosts payload integrating APIs. The APIs are provided being specified before O–ATM deployment. In Figure 1, the neuromorphic computing payload hosts more API interfaces than the communication payload and the GUI.

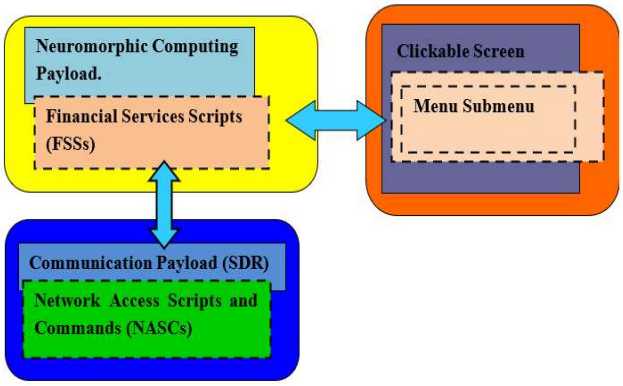

Figure 1 Relations between the components in the O–ATM.

The functional flowchart showing the execution of operations in the O–ATM is shown in Figure 2. The flowchart shown in Figure 2 demonstrates the case of FSS internal loading and FSS external loading. FSS internal loading refers to the case where the ATM of one financial service provider hosts the FSS of other financial service providers. The FSS of the external financial service provider is loaded when the identity of the concerned external financial service provider is selected by an individual (i.e. user) at the VDS.

FSS external loading describes the case where the FSS of the requested financial service provider is not available on the requesting ATM. In this case, the NASC of the ATM (owned by a given financial service provider) requests for the FSS of the selected financial service provider. This FSS request is executed by the NASC of the financial service provider that owns the accessed ATM. The execution of external FSS transfer assumes that the computing payload aboard the ATM has sufficient computing resources to host the requested and received FSS.

This is necessary when the ATM is yet to incorporate the computing payload of other financial service providers. In this case, it is suggested that the financial service provider should increase the capacity of the computing and communications payload. This is necessary to provide the capacity required to execute the FSS external loading procedure. In the case where external FSS loading is executed, the concerned financial service provider is notified of the need to install computing and communications payload in the concerned ATM. This is necessary to reduce the incidence of external FSS loading thereby lowering the delay associated with ATM access by the individual. Similar dynamics are associated with the execution of external NASC loading.

In the external NASC loading, the financial service provider is notified to install communication payload with the associated software defined radio (SDR). The SDR is loaded with the pre–configured data communication parameters. The SDR for a given financial service provider hosts operational parameters enabling the connection to different databases. The database holds information for different categories of individuals (with accounts domiciled with a financial service provider). The financial service provider is considered to have a distributed database and server storage system. This is considering the case where the financial service provider does not utilize a cloud computing service provider. The information on individuals with accounts being operated by a financial service provider is stored in a distributed computing platform. The SDR hosts information enabling the access of data from different databases owned and operated by the financial service provider. Each database has different access details and is connected to wireless networks requiring different SDR parameters.

The SDR is crucial to the offering of financial services by the proposed O–ATM. The neuromorphic hardware in enabling the selection of the financial service provider specific FSS also enables the loading of the SDR configuration details. Each financial service provider hosts information on the network connectivity details and hosts this in the FSS. The SDR is suitable for this role as its operational parameters are reconfigurable. The reconfigurable SDR parameters are: (i) short message service servers, (ii) back-up message service servers, (iii) gateway address, (iv) alternate gateway address, (vi) domain name service server address, (vii) alternative domain name service server address, (viii) name of the financial service provider specific transaction databases, and (ix) communication channel encryption mechanisms. The communication channel encryption mechanisms are those that each financial service providers are using in the existing adoption of cloud computing technology. The identified parameters are loaded to the SDR after the neuromorphic hardware triggered reconfiguration. An SDR with a field programming gate array (FPGA) switching latency of up to 15 seconds is feasible. Therefore, a delay of (55–60) secs is expected where the O-ATM's use between users involves different financial institutions.

The relation between the SDR, databases and computing platforms being access is shown in Figure 3. The scenario in Figure 3 shows the case where the O–ATM has two SDRs belonging to two different financial service providers. Each provider has four databases i.e. Database A, Database B, Database C and Database D. In Figure 3, the databases are accessed via different wireless technology protocol implementations necessitating SDR dynamic re–configuration. The required parameters are pre-programmed in the SDR.

The databases belonging to each financial service provider are accessed by the SDR in a bi-directional manner to enable the use of individual data. The networked access is realized via SDR – database connection and maintained while conducting a financial transaction and using the O–ATM. Each database of the financial service provider hosts the profile of all users i.e., banking service clients. The security arises in two steps. First, the wireless link is only maintained when the user is utilizing the O–ATM. Second, the wireless link is encrypted via 5G network encryption standard i.e., the 128–NIA2 (Eleftherakis et al., 2025). The use of the 128–NIA2 encryption solution ensures that information on the wireless link between the O–ATM's SDR and the financial service provider database. Furthermore, the authentication method is the 5G–Authentication and Key agreement that accompanies the 128–NIA2 network encryption standard (Lasierra et al., 2023). The system related attacks such as FSS malware injection, and FSS loading related attacks are also mitigated in the proposed network architecture. The FSS loading process involves

external cloud communication with the O–ATM. This communication is executed via the combination of the 128–NIA2 and 5G–AKA. Furthermore, FSS malware injection is mitigated via the execution of a cloud-based malware scan prior to FSS transfer. The feasibility of using machine learning based solution in this case is realistic as the cloud platform has sufficient computing resources.

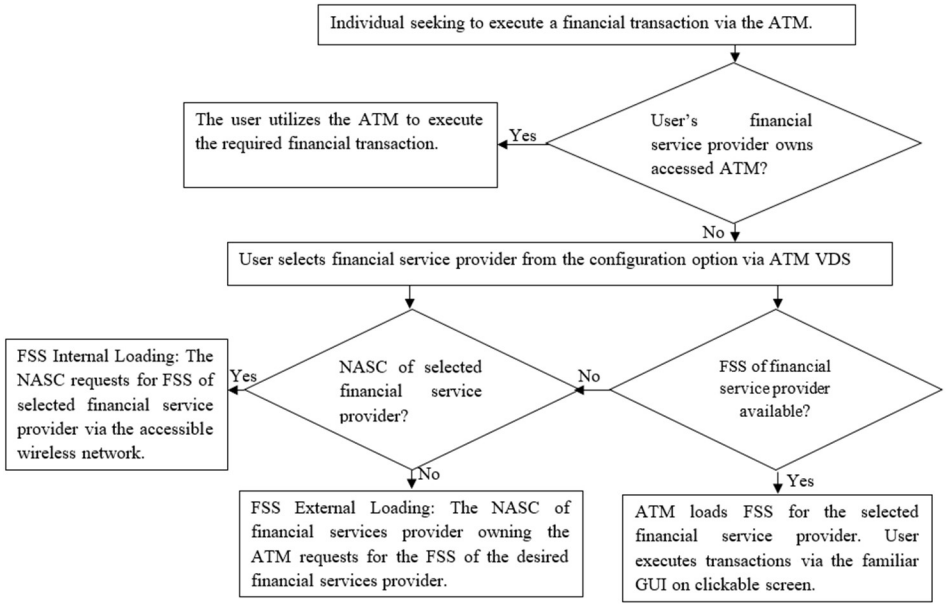

Figure 2 Sequence of operations in the course of conducting a financial transaction in the O–ATM.

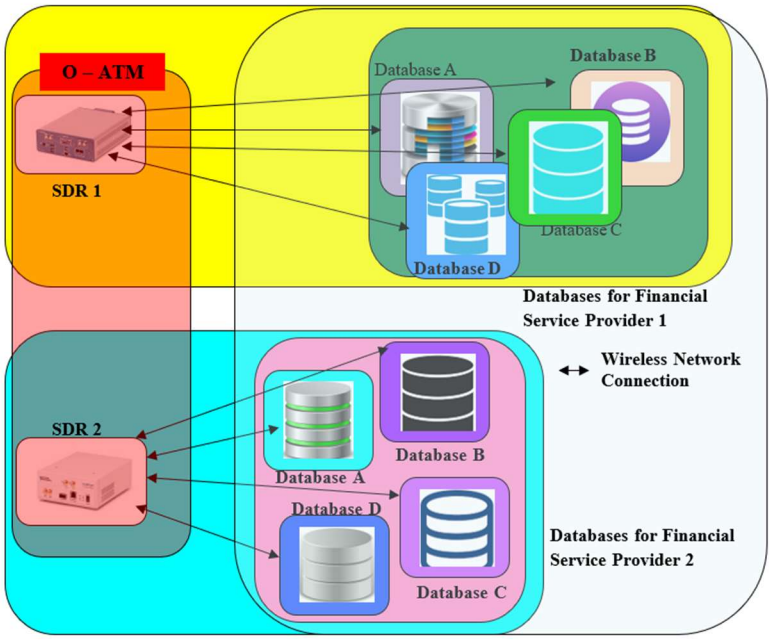

Figure 3 Relations between payload in the O–ATM and databases for financial service providers via a network.

III. Second Aspect: Open-ATM: Role in Enhancing Cloud Computing Service Access

This section addresses the challenge of enhancing access to cloud computing using the O–ATM and is structured as follows. Section A discusses the considered problem. Section B describes the cloud mode operation of the O–ATM. Section C discusses the O–ATM's cloud mode functionality.

A. Description of the Addressed Challenge (s)

Cloud computing platforms offer services in data storage and access. Individuals can store different types of information such as text, image, audio, and video content aboard cloud platforms. The data storage and access services in the cloud computing domain are offered by different service providers such as Amazon, Google, and Microsoft.

In addition, the access to cloud computing services requires that the user has access to a network and a supporting device such as desktop computer, laptop PC, mobile phone, or any device with networking and storage capability. The necessity of having these devices in addition to network access increases the requisite condition and barrier for potential cloud computing service subscribers. Furthermore, the average individual utilizes information and communication technology on a daily basis. However, most individuals are unaware of service offerings and prices across multiple cloud computing service providers. This is important to enable the individual to make a good decision as regards data storage and access via cloud computing platforms.

Therefore, it is important to ensure that individuals without sufficient resources to own data storage devices such as sophisticated smartphones, laptops and desktop computers or individuals in areas with poor or non–robust access to the internet can make use of cloud computing platforms. The individual in this context should also be able to access cloud computing services from different data storage and access service providers. It is important that the individual be able to compare the service access charge for data storage and access from different cloud computing service providers.

B. Proposed Solution: Cloud Mode of the Open–ATM (O–ATM)

A constructive interaction between financial service providers and cloud service providers is beneficial in different aspects such as enabling people to make the necessary payment for cloud computing services. In the current climate of financial innovation, it is not feasible for individuals to make payment for cloud computing services via an automated teller machine. This perspective and innovation do not make the O–ATM to function as a communication node in the current cloud computing and networking ecosystem.

In enabling access to cloud computing service, the O–ATM incorporates an external universal serial bus (USB) port, data compression component and drive plug and play entity. The USB port enables the insertion of storage devices into the O–ATM. This prompts the display of the cloud data access and storage menu options on the O– ATM. The insertion of the drive also activates all the SDRs in the communication payload of the O–ATM being accessed. The O–ATM transits into the cloud mode with the insertion of the USB drive.

The O–ATM has own user menu that is displayed to the individual utilizing the O–ATM. In the cloud mode, the computing payload for all financial service providers with payload aboard the concerned O–ATM is activated. The computing payload hosts the data compression component. The data compression component reduces the size of the data to be transferred to the cloud computing platform. The compressed data is then transmitted in a distributed manner via the activated SDRs to the cloud computing payload. The choice of the cloud computing payload is made by the individual from a menu comprising different cloud computing service providers. The individual intending to store data also selects the payment option i.e. the account from which charges is to be made via the menu option from the O–ATM in the cloud mode. The sequential steps in the O–ATM's cloud mode are:

Insertion of USB Interface Storage Drive: The first step is the insertion of the storage drive i.e. the hard disk drive, flash drive, or any other input storage drive with a USB interface. The insertion of the USB storage drive prompts the O–ATM to transit to the cloud mode.

Preference Selection: In the cloud mode, the O–ATM enables the individual to select preferences as regards data storage options. The selection of preferences enables the individual to select the range of costs associated with the storage of data of varying sizes aboard the cloud computing platform. The user selects a preferred option from the displayed price menu. In addition, the user selects the range of sizes for the files to be updated.

Selection of File(s): The O–ATM selects the file(s) whose storage is desired. These files are selected for future upload to the desired cloud computing service provider.

Confirmation of Selected Service Provider: The O–ATM in cloud mode prompts the individual to select the cloud service provider that meets the individual's preferences.

File Compression: The process of file compression is done by the activated computing payload. The process of file compression is done by the computing payload of each financial service provider. Each computing payload hosts the file compression software. The file compression is conducted in a multi–step process. The multi–step process is shown in Figure 4. The selected files are compressed using compression software such as the Zstandard (.zstd) format. The Zstandard format is considered because of its suitability in banking application programming interfaces (Abdul-Jabbar et al., 2026). The enabling compression software that is pre-loaded aboard the proposed O–ATM. The compression software reduces the file size prior to its transmission to the cloud computing platform of the service provider This reduction of the file size is executed to reduce the data transmission latency for a given network link speed or throughput. A compression ratio of 40% results in a corresponding reduction in the comp.

Activation of Communication Payload: The communication payload for all financial service providers aboard the O–ATM is activated. The SDRs in the communication payload are pre–loaded with configuration parameters enabling them to communicate with cloud computing service provider. The compressed file intended for data storage is sent across multiple wireless paths. The wireless paths traverse mobile wireless networks that have a direct connection to the destination i.e. the cloud computing platform.

The steps listed are executed in a sequential fashion by the O–ATM in the cloud mode. The description considers that the O–ATM in cloud mode utilizes wireless network for transmitting compressed data intended for later storage. The use of wireless networks leveraging on the high speed and low latency transmission is supported in the fifth generation of communication technologies. The fifth-generation communication technology is able to support the realization of the expected low latency data transmission. The use of radio and wireless communications is suitable in cases where there is patchy or zero existence of supporting fibre optic infrastructure.

In a case where there is availability of fibre optic infrastructure, the O–ATM connects to the network entities that provide the link to the destination cloud platform. This is feasible in a context where fiber to the home networks exist. In such a case, connecting the O–ATM to the cloud computing platform is less challenging.

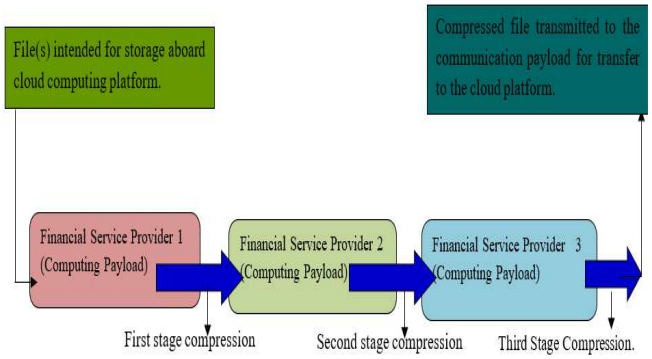

Figure 4 A three-stage compression process suitable for use in the proposed O–ATM in the cloud mode.

C. Functionality of the O–ATM in Cloud Mode

The realization of the O–ATM for cloud mode operation requires the incorporation of new features and capabilities. Besides the data compression, the cloud mode O–ATM requires the incorporation of networking solutions. Networking solutions enable the establishment of connections from the O–ATM to the cloud computing service provider. The cloud mode also incorporates network access scripts and commands (NASCs). The development team of the financial service provider and cloud computing service provider develops these NASCs. The cloud mode NASC comprises access information to the computing platform for different cloud service providers. A cloud mode NASC installed on the communication payload for a cloud service provider comprises information for accessing the platforms of different cloud service providers. The cloud service providers are those having an existing agreement with the financial service provider. Each cloud service provider has separate agreements with the financial service provider in the O-ATM cloud mode. A subscriber selects the desired cloud service provider and stores data with an identifier being issued by the O-ATM. The identifier is used for future data downloads.

In addition, each cloud service provider has own dynamic cloud service interface script (CSIS). Being dynamic, the CSIS can be upgraded by the financial service provider on behalf of the cloud service provider. The CSIS is defined by the software development team of the cloud computing service provider. It comprises storage options being offered by the cloud computing platform to the user or subscriber. The CSIS upgrade enables cloud computing service providers to change the features of the service that they offer to individuals and potential subscribers. This is realized by providing a connection between the cloud computing service provider and the O–ATM. The cloud mode NASCs can be upgraded like the CSIS. The sequence of functions in the O–ATM showing transition between finance and cloud modes is shown in Figure 5. The difference between the existing ATM model and O–ATM is presented in Table 1.

The sequence and transition in Figure 5 consider only the case where the individual only transmits compressed files to the cloud computing platform for data storage. However, it is also possible for an individual to access data via the O–ATM in the cloud mode. In this case, the data access option is included as part of the menu and submenus defined for a cloud computing service provider (defined in the CSIS). In this case, the individual seeking to access a file via the O–ATM is given a content identifier that is transmitted to their mobile device via the internet. The content access is realized in three steps after the O–ATM transitions to the cloud mode. These are (1) Selecting the cloud service provider from whom content access is desired, (2) Choosing the option to access content and (3) Providing the content identifier.

APIs play a crucial role in the O-ATM cloud mode. They enable communications between the neuromorphic computing payload (CSIS, NASC), communication payload (of the O-ATM), and the computing payload. Each of the CSIS and the NASC have communicating APIs with each other for the derivation of configuration information. The communication payload receives the configuration information (SDR related) from the neuromorphic computing payload via the neuromorphic computing payload–communication payload API. The neuromorphic computing payload API also interacts with the USB in the O–ATM cloud mode. Essentially, there are three APIs in the O–ATM cloud mode. These are CSIS–NASC API (implemented in the neuromorphic computing payload) API, Neuromorphic computing payload–communication payload API, and the neuromorphic computing payload–USB interacting API. In the cloud mode, the data is first read from the USB via the neuromorphic computing payload–USB interacting API, the next task is invoking the CSIS–NASC API to determine the reconfiguration parameters for the selected cloud service provider, the communication parameters are sent to the communication payload via the neuromorphic computing payload–communication payload API. This is done alongside the data read from the USB. In a data download session, the first step is an invoking of the neuromorphic computing payload-communication payload API to enable O–ATM downlink execution. The downloaded data is sent to the neuromorphic computing payload via the neuromorphic computing payload-communication payload API. Then, the neuromorphic

computing payload sends the data to the USB via the neuromorphic computing payload–USB API.

The conduct of updates to the O–ATMs' FSS, NASC and CSIS constitute an important operational aspect for the proposed solution. Generally, these updates should be conducted without resulting in significant service disruption. Updates can be conducted during the finance mode and the cloud mode of the O-ATM as indicated in Table 1. The scheduling of the updates is anchored around the O–ATM's usage activity. The updates can be conducted during periods of low usage activity such as mid-night. In addition, the concerned and identified updates can be conducted during daylight periods accompanied with low usage activity. Prior to this period of low activity, updates are configured from an external cloud computing platform before they are committed to the deployed O–ATM. An ATM restart is recommended after installing and applying system component updates.

The need for restart execution is the rationale for scheduling the update during low usage activity period. Furthermore, the O-ATM displays the need to initiate an update and corresponding restart and indicates the introduction of a brief pause in functionality for update download, installation, and execution. The updates to be installed are tested prior at the originating and external network point before O-ATM download, and installation.

The operation of the O–ATM is in line with financial authority standards. This can be seen in that uses 5G authentication, authorization, and encryption for protecting the wireless channel. The use of these authentication, authorization, and encryption mechanisms ensures compliance with general data privacy rules. These also ensures that user details remain private and confidential. In addition, the use of hardware enabling a re-configuration latency of less than 60 seconds considers user tolerance for delay. In addition, the open system provides an avenue for the financial service provider to specify its own interface menu via the FSS MTN specification. The use of the proposed solution does not project the re-issue of ATM cards for the rationale of supporting backward integration. Furthermore, the O-ATM functioning in the cloud mode should be designed to ensure that users are issued with unique identifiers and are associated with file upload completions. The unique identifiers are types of one-type pin that can later be used for data access and download when applicable. In addition, the download and upload latency should not exceed a minute to limit queuing duration for other users.

IV. PERFORMANCE ANALYSIS

The discussion in this section presents the performance analysis and simulation results in the first aspect, and second aspect, respectively. The formulated performance metrics are the ATM–financial service provider density (ATM -FSD), and the cloud service access reach (CSAR). The ATM-FSD and the CSAR are service-related metrics associated with the O–ATM.

A. First Aspect – Performance Formulation

The use of the proposed O–ATM model is beneficial in two respects. The first is that the hosting of multiple financial institutions increases the ATM density for each financial institution. This is realized without increasing the number of physically deployed ATMs. This benefit arises because the proposed approach enables a financial service provider to have their financial services accessible at a location via the provisioning of FSS and NASC provisions. This is realized in a manner that enhances the hosting capability of third-party managed ATM systems.

In this regard, the formulated metric is the ATM financial service provider density (ATM-FSD). The second benefit arises because of the O-ATM cloud mode which results in an increased reach for cloud data uplink and data downlink process. The formulated metric is the cloud service access reach (CSAR).

Let the set of financial institutions be given as β such that:

$$\beta = \{\beta_1, \beta_2, \dots, \beta_A\} \quad (1)$$

The a^{th} financial institution, $\beta_a, \beta_a \in \beta$ is hosted aboard the b^{th} ATM, $\alpha_b, \alpha_b \in \alpha, \alpha = \{\alpha_1, \alpha_2, \dots, \alpha_B\}$ such that the set of financial institutions hosted aboard α_b at the epoch $t_y, t_y \in t, t = \{t_1, t_2, \dots, t_Y\}$is denoted:

$$\alpha_b(\beta, t_y) = \{\alpha_b(\beta_1, t_y), \alpha_b(\beta_2, t_y), \dots, \alpha_b(\beta_A, t_y)\} \quad (2)$$

In addition, the indicator that the a^{th} financial institution, β_a is present aboard the b^{th} ATM, α_b is denoted $I\left(\alpha_b(\beta_a, t_y)\right) \in \{0,1\}$. The a^{th} financial institution, β_a's services are present and not present aboard the b^{th} ATM at the c^{th} location $l_c, l_c \in l, l = \{l_1, l_2, \dots, l_C\}$ when $I\left(\alpha_b(\beta_a, l_c, t_y)\right) = 1$, and $I\left(\alpha_b(\beta_a, l_c, t_y)\right) = 0$, respectively. A presence implies the availability of the FSS, NASC and CSIS. In the existing case, the ATM-FSD, Γ_1 is given as:

$$\Gamma_1 = \sum_{b=1}^{B}\sum_{a=1}^{A}\sum_{c=1}^{C}\sum_{y=1}^{Y} N\left(\alpha_b(\beta_a, l_c, t_y)\right) \Big| I\left(\alpha_b(\beta_a, l_c, t_y)\right) = 1 \Big| \quad (3)$$

$N\left(\alpha_b(\beta_a, l_c, t_y)\right)$ are the number of services associated with the a^{th} financial institution, β_a is present aboard the b^{th} ATM, α_b at the epoch t_y.

In the proposed case, the ATM-FSD, Γ_2 is given as:

$$\Gamma_2 = \sum_{b=1}^{B}\sum_{a=1}^{A}\sum_{c=1}^{C}\sum_{y=1}^{Y}\sum_{x=\{CSIS,FSS,NASC\}} N\left(\alpha_b(\beta_a, l_c, t_y)\right) \Big| I\left(\alpha_b(\beta_a, l_c^x, t_y)\right) = 1 \Big| \quad (4)$$

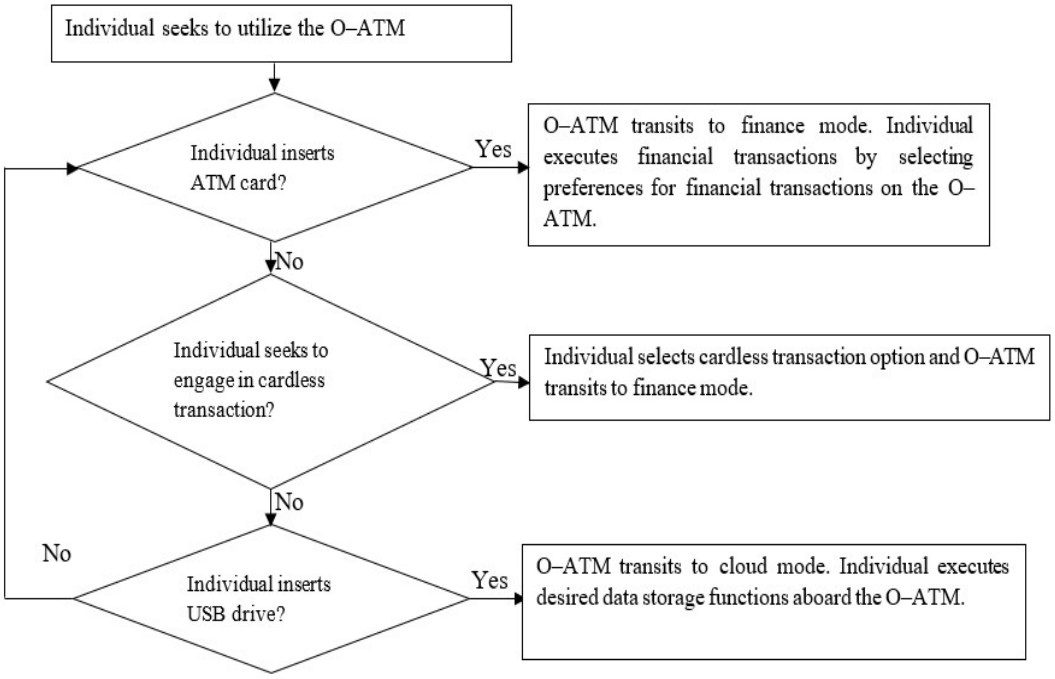

Figure 5: Flowchart showing transition between the finance mode and cloud mode in the proposed O-ATM.

Table 1: Differences in capabilities between the Existing ATM and the O–ATM.

S/N	Criteria	Existing ATM	Proposed O–ATM
1	Participating Entities	Financial Service Providers and Telecommunication entities	Financial Service Providers, Telecommunication entities, and Cloud Computing Service Providers
2	Service Capabilities	Single Financial service provider's tailor specific services.	Multi-financial service provider's custom specific services, data upload, and access in cloud computing.
3	SDR Incorporation	No	Yes
4	Neuromorphic computing payload	Maybe	Yes
5	Number of supported industries	One (Banking and Financial Services Industry)	Two (Banking and Financial Services Industry; and Cloud Computing Service Industry)
6	Funding Entities	Financial service provider(s)	Financial Service provider(s) and Cloud computing service provider(s).
7	Operating Modes	1 (Finance Mode)	2 (Finance Mode and Cloud Mode)
8	External USB port	No	Yes
9	Crowdfunding Scale	Large	Very Large
10	Number of access codes	2 (ATM Card Pin, Cardless Cash Access Transactions Code)	3 (ATM Card Pin, Cardless Cash Access Transactions Code and Content Identifier)

$l_c^x, x = \{CSIS, FSS, NASC\}$ describes the location-specific presence of the entity x.

$I\left(\alpha_b(\beta_a, l_c^x, t_y)\right) \epsilon$ {0,1}is the location specific presence indicator of the entity $x, x = \{CSIS, FSS, NASC\}$ for the a^{th} financial institution, β_a is present aboard the b^{th} ATM, α_b. The entity x is present and is not present at the location, l_c for the a^{th} financial institution, β_a is aboard the b^{th} ATM when $I\left(\alpha_b(\beta_a, l_c^x, t_y)\right) = 1$, and $I\left(\alpha_b(\beta_a, l_c^x, t_y)\right) = 0$, respectively.

The proposed cloud service access reach CSAR is formulated considering the reach of cloud computing based services. Let the set of cloud service providers be denoted θ such that:

$$\theta = \{\theta_1, \dots, \theta_D\} \quad (5)$$

Each cloud service provider has its services accessible via wireless networks across different locations. The location specific cloud service provider indicator is denoted $I(\theta_d, l_c, t_y) \epsilon \{0,1\}$. The d^{th} cloud service provider $\theta_d, \theta_d \epsilon \theta$ is accessible and not accessible from location l_c at the epoch t_y when $I(\theta_d, l_c, t_y) = 1$, and $I(\theta_d, l_c, t_y) = 0$, respectively. The CSAR in the existing and proposed case are denoted ϕ_3, and ϕ_4 respectively:

$$\phi_3 = \sum_{b=1}^{B}\sum_{a=1}^{A}\sum_{c=1}^{C}\sum_{y=1}^{Y} N(\theta_d, l_c, t_y)\left|I(\theta_d, l_c, t_y) = 1\right| \quad (6)$$

$$\phi_4 = \sum_{b=1}^{B}\sum_{a=1}^{A}\sum_{c=1}^{C}\sum_{y=1}^{Y} N(\theta_d, l_c, t_y)\left|I(\theta_d, l_c, t_y) = 1\right| + N(\theta_d, l_{c=O-ATM}, t_y)\left|I(\theta_d, l_{c=O-ATM}, t_y) = 1\right| \quad (7)$$

$N(\theta_d, l_c, t_y)$ is the number of cloud services from the cloud service provider θ_d available at the location l_c and epoch t_y.

$N(\theta_d, l_{c=O-A}, t_y)$ is the number of cloud services from the cloud service provider θ_d available at the location l_c and epoch t_y due to the presence of the proposed O-ATM.

B. Second Aspect – Performance Evaluation

The discussion related to the performance evaluation is presented in this aspect. The performance evaluation is done via simulation using the parameters in Table 2.

S/N	Parameter	Value
Simulation of the ATM-FSD Metric		
Existing Case – Use of only Existing ATMs.		
1	Number of Conventional ATMs	15
2	Minimum Number of Services	0.406
3	Mean Number of Services	2.5258
4	Maximum Number of Services	4.6469
5	Number of Location ATM area	15
6	Number of Areas with Existing ATM	8
7	Number of Areas without Existing ATM	7
Proposed Case – Inclusion of O – ATMs with Existing ATMs.		
8	Number of Proposed O-ATMs	5
9	Number of Areas with Proposed O-ATMs	4
10	Number of Areas with Existing ATMs	11
11	Number of Existing ATMs	10
12	Minimum Number of Services	1.532
13	Mean Number of Services	2.828
14	Maximum Number of Services	4.088
15	Minimum Number of Services – O-ATM	5.502
16	Mean Number of Services – O – ATM	7.149
17	Maximum Number of Services – O – ATM	9.390
Simulation of the CSAR Metric		
Existing Case		
18	Number of considered and existing ATM locations	15
19	Number of locations with ATM being present	7
20	Number of locations with ATM absent	8
21	Minimum number of services – Existing ATM	0.0979
22	Mean number of services – Existing ATM	2.3652
23	Maximum number of services – Existing ATM	4.4389
Proposed Case		
24	Number of considered and proposed O–ATM locations	5
25	Number of locations with the O–ATM being present	5
26	Number of considered and existing ATM locations	10
27	Number of locations with existing ATM being present	5
28	Minimum number of services – existing-ATM	0.8363
29	Mean number of services – existing-ATM	3.3993
30	Maximum number of services – existing -ATM	4.9494
31	Minimum number of services – O-ATM	1.4701
32	Mean number of services – O-ATM	4.4486
33	Maximum number of services – O-ATM	8.4007

The simulation scenario being considered is one where existing ATM and the proposed O-ATM can be deployed in a varying number of locations. However, only one ATM (existing and proposed) can be deployed in each location. In addition, each ATM has a variable number of services. This enables the consideration of ATM with varying performance and service capabilities. This is done to ensure that the simulation considers different types of ATMs with varying service capabilities. The results of the ATM-FSD for the existing case and proposed case obtained via simulation is presented in Figure 6. The use of the proposed solution (in the proposed case) enhances the ATM-FSD instead of the existing case by an average of 21.2%. This implies that the use of the proposed O-ATM where the presence of the FSS, and NASC related scripts signify financial service provider positioning instead of physical ATM deployment enhances the ATM deployment density for multiple service

providers. Furthermore, the results of the CSAR metric for the existing case and proposed case is presented in Figure 7. The use of the proposed solution (in the proposed case) enhances the CSAR instead of the existing case by an average of 63%. This implies that the use of the proposed case i.e., incorporating the data access in a deployed ATM machine increases cloud service coverage.

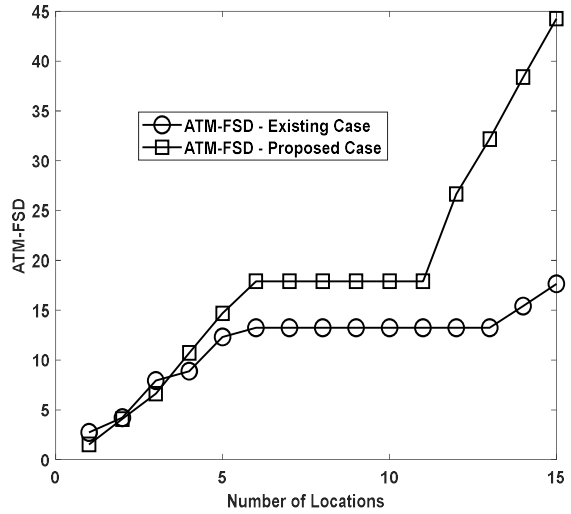

Figure 6 Simulation results for the ATM-FSD performance metric.

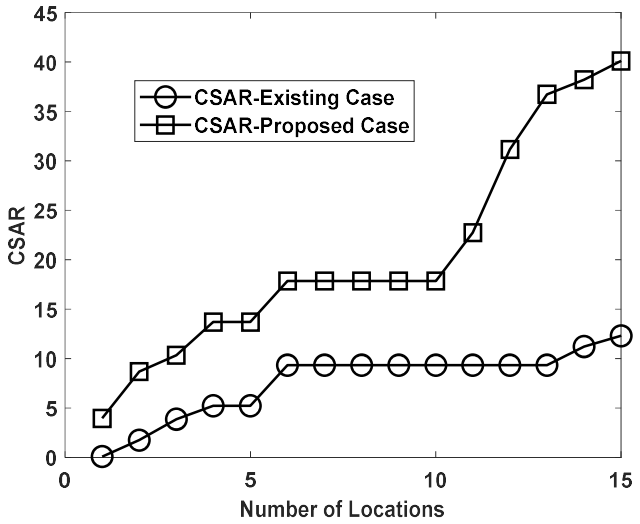

Figure 7 Simulation results of the CSAR performance metric.

V. CONCLUSION

The paper describes the open–automated teller machine (O–ATM) for future financial transactions and cloud content operations. It recognizes the increasing growth in the sophistication of individual demand when accessing financial services via the automated teller machine. The discussion opines that the automated teller machine can meet the increasing functional demands of individuals i.e. users. In addition, the future automated teller machine is recognized to be capable of enhancing access to cloud computing services at the level of the retail consumer or user. The discussion has considered the description of innovative advances to the current automated teller machine. This has led to the emergence of the newly proposed open–automated teller machine. The discussion slightly deviates from the existing approach of hinging on advanced software to realize new and novel technologies. In the existing approach, the use of virtual machines hosted on centralized hardware in the considered technological solution is a common pathway. The solution described here is one in which non–centralized hardware is utilized in the proposed automated teller machine model. The proposed solution of the proposed O-ATM is considered non-centralized as it has multiple interacting components. i.e., the ATM, and cloud computing aspect for configuration data access and user data access. Each aggregation of non–participating actors contribute centralized hardware that desire to host a feasible operation instance on the proposed automated teller machine. The discussion considers the automated teller machine as a communication node enabling data-based services while leveraging on advances in cloud computing platform technology. In addition, performance analysis is also evaluated via simulation related analysis. In addition, performance analysis shows that the use of the proposed O-ATM enhances the ATM deployment density and cloud service reach by an average of 21.2%, and 63%, respectively.

AUTHOR CONTRIBUTIONS

A.A Periola: conceived and managed the project, designed the research, executed formal analysis, and processed data. A.A Alonge carried out peer review, and project administration. K.A Ogudo: co-supervision, assisted with research design, analysis, carried out peer review, and project administration.

ACKNOWLDGEMENT

The authors wish to extend their sincere gratitude to the Cape Peninsula University of Technology, Tshwane University of Technology, and the University of Johannesburg.

REFERENCES

K. Velayuthapandian, N. Murugan, and S. Paramasivan (2024). End-to-End CNN conceptual model for a biometric authentication mechanism for ATM machines. Discover Electronics, vol. 1, no. 1, Nov. 2024, doi: https://doi.org/10.1007/s44291-024-00034-x.

S. Carbó-Valverde and F. Rodríguez-Fernández (2014). ATM withdrawals, debit card transactions at the point of sale and the demand for currency. SERIEs, vol. 5, no. 4, pp. 399–417, Apr. 2014, doi: https://doi.org/10.1007/s13209-014-0107-9.

J.Ciaccio, and I.Onat (2025). An Analysis of ATM and Point of Sale Skimming. , Orion Forum Cyber Security and Info Technologies, April 25, 2025.

Kizito Paul Mubiru and M. N. Ssempijja (2024). 'Modelling and optimization of ATM cash-loading under

stochastic demand" Discover Analytics, vol. 2, no. 1, Sep. 2024, doi: https://doi.org/10.1007/s44257-024-00023-0.

M. Suder, Tomasz Wójtowicz, R. Kusa, and H. Gurgul (2022). "Challenges for ATM management in times of market variability caused by the COVID-19 pandemic crisis," Central European Journal of Operations Research, vol. 31, no. 2, pp. 445–465, Nov. 2022, doi: https://doi.org/10.1007/s10100-022-00816-2.

M. Ayamga, B. Tekinerdogan, and A. Kassahun (2021). "Exploring the Challenges Posed by Regulations for the Use of Drones in Agriculture in the African Context," Land, vol. 10, no. 2, p. 164, Feb. 2021, doi: https://doi.org/10.3390/land10020164.

O.Akinradewo, C.Aigbavboa, C.Emere, D. O. Ebiloma, O.Akinshipe, and A.Oke (2024). "Barriers to the Adoption of Unmanned Aerial Vehicles for Construction Projects in South Africa," vol. 11, pp. 12–12, Oct. 2024, doi: https://doi.org/10.3390/engproc2024076012.

A.O.Daoud, A. F. Kineber, N. Chileshe, A.Elmansoury, and Khaled (2025). "Investigating barriers to drones implementation in sustainable construction using PLS-SEM," Scientific Reports, vol. 15, no. 1, Jun. 2025, doi: https://doi.org/10.1038/s41598-024-76470-2.

M. E. Rana and L. Z. Ji (2023). "The Role and Potential Applications of Cloud Computing in the Banking Industry" IEEE Xplore, Jan. 01, 2023. https://ieeexplore.ieee.org/document/10099662/ .

E. Greene (2018). "NAB and Microsoft leverage AI technology to build card-less ATM concept - Source Asia (2018), Source Asia, Oct. 21, 2018. https://news.microsoft.com/source/asia/2018/10/22/nab-and-microsoft-leverage-ai-technology-to-build-card-**less-atm-concept/ (accessed Jul. 02, 2025).**

SBS (2023). "The Future of ATM Applications - SBSinnovate," Sbsinnovate.com, 2023. https://www.sbsinnovate.com/en/blog/the-future-of-atm-applications-how-modern-technology-is-transforming-cash-transactions (accessed Jul. 02, 2025**).**

H.Patil, V.Mahandule, L.Khachane, and S. Narkehde (2024). 'Multi-Banking ATM Services using biometrics,' Management Science Letters, Vol..14, 2024, pp 219 – 226.

F. Rahaman Chowdhury, M. Masum Alam Nahid, F. Chowdhury, M. Masum, U. Cali, and M. Sadek Ferdous (2025). "Self-Sovereign Identity Empowered Automated Teller Machines," IEEE Access, vol. 13, pp. 203444–203480, 2025, doi: https://doi.org/10.1109/access.2025.3638625.

F. A. Nafis, M. Fahomida, Md. S. Sakib Alvi, and S. T. Salim Rafid (2025). "SBIoT-ATM: Secure Blockchain-IoT Framework for Next-Generation Automated Teller Machine Security," 2025 28th International Conference on Computer and Information Technology (ICCIT), pp. 1720–1725, Dec. 2025, doi: https://doi.org/10.1109/iccit68739.2025.11490155.

P.Sergiv, B.Dmytro, and S.Yevheniia (2025). "Using the video channel of ATM devices to enhance the level of cybersecurity during customer interactions," Management of Development of Complex Systems, no. 64, pp. 171–176, 2025, doi: https://doi.org/10.32347/2412-9933.2025.64.171-176.

J. Garcia(2025). "A Comprehensive Study on the Implementation of Fingerprint-Based Biometric Systems in ATMs for Secure and Efficient Banking Transactions," Ssrn.com, May 2025, doi: https://doi.org/10.2139/ssrn.5328051.

T. Paul (2025). "Internet of Things and 5G are the revolution to the banking industry using neuro-fuzzy technique," Discover Computing, vol. 28, no. 1, May 2025, doi: https://doi.org/10.1007/s10791-025-09543-z.

O. Runsewe, O. S. Osundare, S. Olaoluwa, and L. Anthony (2024). "Optimizing user interface and user experience in financial applications: A review of techniques and technologies," World Journal of Advanced Research and Reviews, vol. 23, no. 3, pp. 934–942, Sep. 2024, doi: https://doi.org/10.30574/wjarr.2024.23.3.2633.

A. Ali (2025). "Fintech & Digitilization of Banking: User Experience (UX) and User Interface (UI) of Fintech Apps Chair of Banking and Finance Influence of UX/UI Design on User Satisfaction and Engagement in Pakistani Fintech Apps," Jan. 2025, doi: https://doi.org/10.13140/rg.2.2.12301.65765.

S. Xu, L. Jiang, and B. Gu (2025). "Design and Validation of a Smart Neuromorphic System Architecture for Algorithmic Trading," Proceedings of the 2nd International Symposium on Integrated Circuit Design and Integrated Systems, pp. 127–136, Sep. 2025, doi: https://doi.org/10.1145/3772326.3774721.

Stavros Eleftherakis, Domenico Giustiniano, and N. Kourtellis (2025). "SoK: Evaluating 5G-Advanced Protocols Against Legacy and Emerging Privacy and Security Attacks," pp. 196–210, Jun. 2025, doi: https://doi.org/10.1145/3734477.3734716.

O. Lasierra, Gines Garcia-Aviles, E. Municio, A. Skarmeta, and X. Costa-Pérez (2023). "European 5G Security in the Wild: Reality versus Expectations," WiSec '23: Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Pages 13 – 18,May 2023, doi: https://doi.org/10.1145/3558482.3581776.

S. S. Abdul-Jabbar, S. N. Kadhim, A. H. Alharbi, M. M. Eid, and E.-S. M. El-kenawy (2026). "A new secure approach for AI-based compression across various domains," Scientific Reports, May 2026, doi: https://doi.org/10.1038/s41598-026-50271-1.