Received: 24 January 2026 | Revised: 22 June 2026 | Accepted: 27 July 2026 | Published online: 11 August 2026

RESEARCH ARTICLE

Artificial Intelligence and Applications
2026, Vol. 00(00) 1–13
DOI: 10.47852/bonviewAIA62029196

BON VIEW PUBLISHING

An AI-Assisted Timed-Release Encryption Framework for Enhancing Telecom Customer Data Security

Waleed A. Hammood[1], Noor Akma Abu Bakar[2,3,*], Salwana Mohamad Asmara[4], Surizal Nazeri[2,3], Ejiro U. Osiobe[5], Omar Abdulmaged Hammood[6], Marshima Mohd Rosli[7] and Salah A. Aliesawi[8]

[1] *Department of Information Technology, University of Anbar, Iraq*

[2] *College of Computing & Informatics, The National Energy University, Malaysia*

[3] *Institute of Information & Computing in Energy, The National Energy University, Malaysia*

[4] *Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Malaysia*

[5] *Ane Osiobe International Foundation, USA*

[6] *Faculty of Information Technology, University of Fallujah, Iraq*

[7] *Institute for Pathology, Laboratory and Forensic Medicine, MARA University of Technology, Malaysia*

[8] *Department of Computer Network Systems, University of Anbar, Iraq*

Abstract: Telecom operators hold massive amounts of sensitive data of their customers, and information about insider misuse, unauthorized access, and premature disclosure of protected content can be logged. Traditional encryption solutions enforce contextual and temporal access-only policies, which are inadequate to cover all aspects needed for comprehensive protection in such environments. This paper proposes an artificial intelligence (AI)-assisted timed-release encryption framework integrating machine learning–based access control with attribute-based encryption (ABE) and time-controlled cryptographic key release, thus enabling intelligent authorization decisions while enforcing strict temporal constraints on data decryption. Experimental evaluation has been carried out using the IBM Telco Customer Churn dataset, having 7,043 records simulating access behavior patterns. Results show that the proposed approach achieves 94% access control accuracy, reducing unauthorized attempts to 5.2%, far better than conventional AES-256 and ABE methods (performance improvement statistically significant ($p < 0.01$). An AI-driven access control module managed to hit an F1-score of 94.6% for spotting unusual access behavior. Experimental results provide evidence that AI-timed-release encryption presents a scalable, practical solution to enhance telecom customer data security with computational overhead within acceptable limits for modern telco environments. This makes it suitable to be deployed in such environments.

Keywords: artificial intelligence, information technology, data security, telecom customers, application

1. Introduction

Telecommunications companies collect, store, and process massive volumes of personal and behavioral customer data for billing optimization of services and other values they may wish to add proactively to the customer. This has created a huge exposure to cyber threats/internal attacks and violations of privacy that might be committed deliberately or accidentally by an employee within the organization itself [1]. Regulations are pushing for more enhanced mechanisms on how protected private information should be, thus driving telecom operators into deploying new advanced security solutions. Traditional encryption only covers data at rest and in transit. It has no support for contextual access controls or time-based restrictions [2]. The issue of insider misuse remains because traditional systems allow access within approved purposes and timeframes. Artificial intelligence (AI) is mostly viewed as a tool for adaptive security decisions and intelligent access based on contextual attributes such as user behavior.

***Corresponding author:** Noor Akma Abu Bakar, College of Computing & Informatics, The National Energy University, Malaysia and Institute of Information & Computing in Energy, The National Energy University, Malaysia. Email: Noor.akma@uniten.edu.my

© The Author(s) 2026. Published by BON VIEW PUBLISHING PTE. LTD. This is an open access article under the CC BY License (https://creativecommons.org/licenses/by/4.0/).

Businesses that handle personal data must give considerable thought to protecting it as a privacy concern. Laws and regulations that protect privacy as a human right also mandate that companies put in place the necessary protections. Telecoms have been collecting customer data for decades, but because of the recent emphasis on big data, the processes involved are still getting a lot of attention. Customers are concerned about how these data were obtained, the data points that were captured, and the purposes for which they were intended. With a planned release, timed-release encryption aims to "send a message into the future." One way to do this is by encrypting a message so that the recipient cannot decode the ciphertext until a certain future time. To prevent a dishonest auctioneer from opening bids earlier in a sealed-bid auction, to prevent early vote opening in electronic voting schemes, and to delay the verification of a signed document in settings and on telecom sites are some examples of practical applications for such a primitive [3, 4]. Data security impacts both businesses and consumers since, regardless of the industry, data breaches remain one of the worst threats to customer safety and business continuity. Because of this, it's essential to maintain trust and loyalty by being forthright and truthful about the data collection techniques [5]. Customers know that telecom firms collect data to bill them, but as these methods get more complex, all of these companies will need to give customers clear privacy policies if they want to keep control over their personal information. Telecom networks use AI technologies and machine learning (ML) to improve security and network performance and personalize user experiences [6]. In the telecommunications industry, certain personal data are collected without our awareness or agreement. Search engines, Internet access, localization, and online activities, including website visits and keyword input into mobile devices, all leave behind traces that may be monitored and recorded for a number of uses. These technologies enable intelligent customer service solutions that ultimately boost efficiency and please clients. Because telecom firms are so competitive, predicting and managing churn is clearly one of the largest issues they face. However, a variety of ML techniques are used to help a mobile business retain its customers. Certain ML approaches are appropriate for specific data mining applications, such as image processing, speech recognition, and fraud detection, depending on their specific objectives. This demonstrates how data mining, an ongoing process that is equally crucial to data science, depends on ML [5]. The digital age saw the development of several modern technologies, including AI, ML, and data mining. A distinguishing characteristic of the telecom sector is the ability of mobile carriers to leverage "Big Data" from customer data to do various studies to forecast client attrition. Researchers can use ML algorithms, such as neural networks, and statistical ML algorithms such as Decision Trees, Random Forest, K-Nearest Neighbors, and Linear Regression, to identify patterns in data. These patterns aid in data classification, prediction, and, in the end, the development of a suitable model based on that specific dataset [7]. The stages of the customer life cycle typically comprise acquisition, build-up, peak, decline, and churn, according to observations. The procedures for creating, storing, distributing, and managing information are now rapid and easy. But these advancements have also inevitably made information more vulnerable. Adversaries are now using network-oriented warfare in telecom malware programs. Information infrastructures have become the prime target of malware writers. The more severe hacking attempts have caused harm and even destruction to mobile customers. These days, mobile technology is a network of interconnected information sources that let users interact with the market, access online banking, and conduct transactions. AI-driven telecommunications security systems currently available have primarily focused on three types of security: metadata anomaly detection, intrusion identification, and behavioral monitoring. Each of these telecommunication security approaches does provide the standard level of confidentiality protection implemented by standard cryptographic algorithms (such as AES) and/or attribute-based encryption (ABE). However, these algorithms do not provide intelligent contextual authorization or adaptive behavioral validation. Additionally, most existing timed-release encryption methods provide delayed access to data; however, the information has not been subject to AI-driven behavioral analysis to help prevent insider threats. Therefore, there is a significant gap in the current research literature on integrating intelligent authorization, fine-grained cryptographic access control, and temporal enforcement within one comprehensive telecom security structure. To eliminate this research gap and advance the security of telecom systems, the proposed AI-assisted timed-release encryption (AI-IDTRE) framework combines AI-driven behavioral authorization (ABE) and timed-release key management into a single architecture that prevents unauthorized access, insider misuse, and premature data disclosure at the same time.

This paper proposes an AI-IDTRE framework wherein ML access control is combined with time-based encryption. Therefore, this composite framework supports a scheme in which data can only be decrypted by authorized entities within temporal constraints, purely defined by the data owner [8].

1.1. Motivation

Telecommunications is one of the fastest industries to embrace digital transformation. This has led to a huge increase in the amount of sensitive customer data stored and transmitted across various systems. Personal details, billing information, logs of communication, and details of service usage make telecom infrastructures very attractive to attacks and unauthorized access.

Traditional encryption technologies can ensure high levels of data confidentiality but do not provide intelligent access control or temporal enforcement mechanisms. For example, in most practical scenarios, access to sensitive telecom data should be based not only on user credentials but also on other contextual factors like access behavior, user role, and timing constraints. Dynamic security requirements of this type cannot be met by static access control mechanisms.

Furthermore, insider threats and unauthorized premature access to sensitive information are still major issues in telecom environments. Thus, there is a security framework that would very well combine intelligent decision-making with tight temporal restrictions. This, therefore, is what motivated the development of the proposed AI-IDTRE framework, which marries ML-based access control with cryptographic protection to enhance telecom customer data security.

The rest of this paper is organized as follows. Section 2 gives the literature review and discusses existing related work in timed-release encryption, ABE, and intelligent access control mechanisms. Section 3 describes the proposed AI-IDTRE framework. Section 4 gives the methodology and implementation details. Section 5 discusses the experimental results and performance evaluation. We end with Section 6, which concludes the paper and outlines future research directions.

2. Literature Review

Most of the work done previously in telecom data security was based mainly on encryption schemes and access controls while proposing AI-based anomaly detection as well. It has been found that the widely adopted ABE to enforce fine-grained access control contains no temporal constraints. Timed-release encryption has been proposed for delayed data access; however, intelligent decision-making about data access is still in its nascent stage of development. Behavioral analytics have proven their efficiency in the detection of abnormal behavior and insider threats within organizations. Therefore, most existing approaches either address intelligent detection or encryption separately. Table 1 presents some major limitations of the existing works. None has proposed an integrated AI-driven timed encryption framework specifically for a telecom environment [6].

AI-assisted technologies have the potential to replicate human cognitive functions, such as learning and problem-solving. AI may therefore collect, examine, and identify data prior to performing particular tasks. AI enables human-like tasks and ML. AI may be divided into two broad categories: strong AI and weak AI. Artificial general intelligence, or strong AI, refers to a more complex and advanced computer that possesses awareness, sensitivity, and a mind that exhibits intelligence in several areas and is able to do a wide range of tasks. However, weak AI, also referred to as artificial narrow intelligence, is a very basic system that performs a restricted number of tasks, such as self-driving automobiles. Infrastructure security is prioritized over privacy in the telecommunications sector despite the fact that privacy has been extensively studied in the health sector. The ability of AI techniques to function constantly in the background and make decisions in real time for private and sensitive customer data is one of their advantages [9]. This poses a fascinating research question: How may AI enhance the prediction of company failure? It is crucial to remember that telecommunications operations employ private and sensitive consumer data to deliver services to end customers [10]. Businesses may be able to utilize more information to customize marketing efforts if ecosystem partners share data. However, companies are also exposed to greater data security concerns when sharing data with ecosystem partners, which may deter privacy-conscious consumers from using AI-enabled marketing and limit data exposure that may boost AI's value. Telecom has to develop privacy and AI governance norms, particularly in view of research showing potential risks associated with integrating AI with interactive data security [9]. One of the many problems with the modeling techniques used to predict data breaches for data security and telecommunications sites is classification performance [11]. This leads to malicious users, especially when the algorithm anticipates that data will migrate through data breaches and misclassifies private customer information. As a result, privacy and security are compromised [12]. Telecommunications companies need this information for a number of reasons, such as churn prevention, financial stability preservation, and risk management research [13]. Such data must be comprehensive, rational, and available whenever tasks pertaining to the time management process call for them. Thus, one of the most important survival strategies in the home appliance rental sector is predicting the probability of client attrition [14]. Nonetheless, there may be a chance for data-driven customer attrition prediction modeling research in the home appliance rental sector. The two main technological challenges are class imbalance problems and classification algorithms' prediction performance. In the past, researchers employed single categorization approaches to forecast customer turnover; more recently, ensemble-based classification algorithms have been developed. The increasing speed of data creation affects every aspect of our lives. Everybody in this situation, individuals, governments, and businesses, needs to strengthen their data security protocols. Data loss or theft is becoming a major financial problem as more business activities are moved online and as more businesses and consumers go online internationally. There are several causes of data security incidents. These include, but are not limited to, system failures, malware or virus infestations, employee theft or fraud, and unauthorized third-party attacks. Historically, companies whose business plans center on generating revenue from data processing and storage have been the most vulnerable [15]. Therefore, IT service providers and resellers that handle large volumes of specialized data were the main victims or targets of data breaches. Without compromising the same level of information analysis, every telecom company seeks to increase data security and privacy. Data secrecy is essential since the data are being moved between the cloud computing resources and the smart system. Businesses need to believe in the model to some extent in order to use the data. Table 1 shows the comparison of existing related works.

2.1. Research gap

While several studies have examined the use of AI for intrusion detection and encryption for telecommunications security, very few have addressed the need for an intelligent behavioral access control system that also utilizes temporal cryptographic protection within an integrated framework. Existing AI security systems rely primarily on anomaly detection and policy enforcement but do not incorporate any form of cryptographic control

Table 1
Comparison of existing related works

Reference	Method	Strength	Limitation
Imura, Y. and Emura, K. (2025)	Timed-Release Encryption	Introduced time-controlled decryption	No intelligent access control
Lu, G. et al (2025)	Attribute-Based Encryption	Fine-grained access control	No temporal restriction
Recent ML-based Access Control	AI/ML Security	Intelligent authorization decisions	No encryption integration
Existing Hybrid Encryption Models	Combined Security Methods	Strong cryptographic protection	Limited AI integration
Proposed Work	AI + ML + ABE + TRE	Intelligent, adaptive, and time-controlled security	Addresses existing limitations

over when information can be released. In contrast, timed-release encryption technology is primarily focused on delaying decryption and does not provide any means to adaptively authorize access based on contextual evidence related to insider abuse or abnormal access behavior. The new AI-IDTRE framework improves the security of telecom customers' data by combining AI-driven behavior analysis as an access control mechanism and timed-release encryption. In addition to fine-grained attribute-based authorization methods for granting access privileges based on user attributes or roles, it has implemented a two-layer approval process with behavioral legitimacy assessments using access duration time restrictions to better detect unauthorized or suspect behavior. Timed-release requirements also significantly reduce the likelihood of releasing sensitive information early, even if the user requesting the information would normally have been granted access. Overall, the AI-IDTRE provides a security framework for telecom that is designed explicitly for high-volume-access, large-scale, dynamic environments.

3. Proposed Framework

This paper proposes a framework of AI-assisted and contextual timed-release encryption that incorporates ML-based intelligent access control with ABE and time-determined key release to address core limitations in traditional timed-release and other encryption systems, mainly regarding insider misuse, premature data access, and lack of contextual authorization, by ensuring that sensitive data can only be accessed by rightful entities within predefined temporal constraints. The main contribution is toward an emerging paradigm of intelligent telecom customer data security at both network and application layers, where AI understands "what," "when," and "who" should get access under dynamically changing contexts spanning across different service providers [1]. This section introduces an AI-IDTRE framework for securing telecom customer data. This is therefore a system of intelligent access control integrated with cryptographic enforcement, carrying temporal constraints on unauthorized and premature access to data. Figure 1 illustrates the overall system architecture together with its data flow.

As in Figure 1, customer data generated by the telecom provider are first passed through an AI-based access control module that checks for legitimate access. The authorized data are then protected using ABE while the corresponding decryption key is protected using time-release encryption. These encrypted data and time-protected key are stored within secure cloud storage such that access will only be granted to authorized users once specific temporal conditions have been satisfied.

For better and easier understanding of how the proposed AI-IDTRE framework works, Figure 2 presents the complete workflow between access decision and timed decryption. The workflow starts when a user sends an access request for telecom customer data that are protected. Behavioral and contextual features are extracted from the request such as frequency of requests, consistency with the user's role, temporal patterns, and device or location information. These features are evaluated by an AI-based access control module (random forest classifier) to check whether this request is legitimate or anomalous. If the access request is classified as legitimate, then check whether the current system time satisfies the predefined release time condition. Implementation of timed-release encryption contains a decryption key release based on an authorization decision and also on a time condition. The released key will be used to decrypt attribute-based encrypted data for secure access to plaintext. In case either access decision or temporal validation fails, deny the request. This workflow shows both intelligent authorization and cryptographic enforcement of time working together to stop unwanted and premature access. As shown in Figure 2, access is granted only after the AI model decision and time validation stages are satisfied.

3.1. Framework overview

AI-IDTRE is proposed with a multi-layer security architecture as shown in Figure 1 and explained through its five main components, which are:

a. Telecom Data Owner.
b. AI-based Access Control Module.
c. Attribute-based Encryption Engine.
d. Timed-Release Encryption (IDTRE) module.
e. Secure Cloud Storage.

The telecom provider creates and manages its customer data. It also applies encryption to the data of its customers. An AI-based access control module evaluates every single request before or after storage for accessing the data. Only those access requests that meet both authorization and time constraints are allowed to decrypt protected data.

3.2. Data encryption and attribute assignment

Customer data is encrypted by the telecom provider using ABE. A set of attributes is associated with each data object. Attributes can include items such as user role, department, purpose of access, type of service, and contract status. The attributes define access policies that restrict decryption capabilities only to users whose attributes satisfy the policy.

Formally, let D denote customer data in plaintext and A = {a1, a2,,an} denote the attribute set. The encryption function can be written as:

$$C = \text{EncABE}(D, A) \tag{1}$$

where C is the ciphertext output by the encryption algorithm Enc, and therefore, even if somehow someone gets hold of this encrypted data or file, it will not open unless all attributes required are satisfied in place.

3.3. AI-based access control module

Access rights need to be viewed as an aspect that prevents insider threats and unauthorized access attempts. A contextual

Figure 1
Architecture of the proposed AI-assisted timed-release encryption (AI-IDTRE) framework for telecom data security

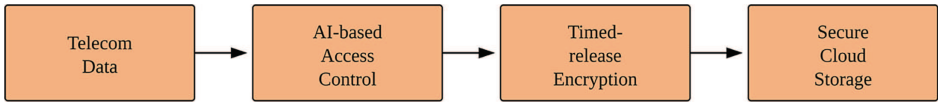
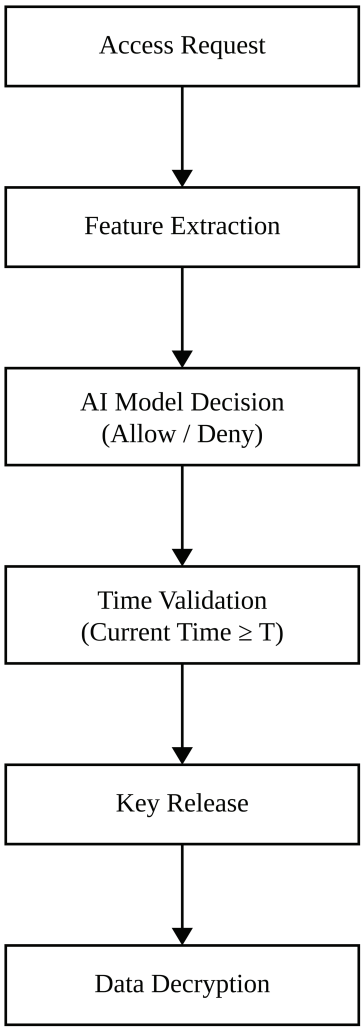


Figure 2
Workflow of the AI-IDTRE access decision and timed decryption process



and behavioral random forest model has been developed, implementing the following features:

a. User's historical information.
b. Frequency of requests made by the user.
c. Time at which a particular request was made.
d. Checking consistency between the role assigned to a user and the roles being assumed within sessions,
e. Device and location details.

The AI engine shall be trained with old log files, both legitimate and malicious entry/request, so that it can automatically identify them in any new entry/request. *R*, the classifier, produces a binary output:

$$\text{Decision}\ (R) \in \{\text{Allow}, \text{Deny}\} \tag{2}$$

Only legitimately classified requests are allowed to pass through the decryption stage. This intelligent filter reduces to a minimum level internal unauthorized access and abnormal behavior exploit attempts.

3.4. Timed-Release Encryption (IDTRE)

The content also includes a description of how time-based restrictions can be imposed even after access authorization using timed-release encryption. The decryption key is encrypted in such a way, by the IDTRE mechanism, that it cannot be released before some predefined time *T*. This helps prevent any premature access to sensitive data and ensures all temporal policies are adhered to. Let *K* be the decryption key and *T* the release time. Then, timed-release encryption is defined as:

$$CK = \text{EncIDTRE}(K, T) \tag{3}$$

The key *K* is made available for decryption only when the system clock satisfies CurrentTime≥T. This proves very useful across telecom environments where access to data must be delayed for auditing, legal, or any operational requirement.

The timed-release mechanism relies on time synchronization that can be trusted. In order to protect against attacks based on manipulation of clocks, it is assumed that trusted time sources, such as secure NTP servers, hardware security modules, or decentralized time validation mechanisms, are available.

Further, multiple time-source verification and audit monitoring can lower the risk of insider manipulation and raise resilience against time-based attacks.

3.5. Dynamic attribute revocation

In real telecommunications scenarios, user attributes can change dynamically, for instance, due to a shift in roles, suspension of account, or termination of employment. Therefore, efficient revocation of attributes is essential for maintaining secure access control. In the framework, access revocation is proposed to be managed through key expiration, periodic key updates, and dynamic rekeying mechanisms. Upon a change in user attributes, the related decryption rights are immediately set to an invalid state to block unauthorized access. This makes sure that revoked users, even if the timed-release condition is satisfied, will not be able to decrypt the protected data. The addition of attribute revocation will enhance both security and adaptability of the proposed access control mechanism in ABE.

3.6. Emergency break-glass protocol

In real telecommunication cases, there can be some emergencies where the data have to be accessed immediately before the scheduled time for release. For example, when law enforcement agents need certain information, for emergency rescue operations, or in situations where a life depends on the information. To cover such scenarios, the proposed framework should include a Break-Glass protocol as an emergency override. In this protocol, temporary access will be provided to very few highly authorized entities after multi-level approval and upon cryptographic check with complete and strict audit logging. Log and track all emergency access events to ensure responsibility and prevent abuse. This function keeps all the security advantages of IDTRE while allowing some freedom in operations when it comes to high-priority situations.

3.7. Secure data storage and access workflow

Once encrypted, the ciphertext, together with the timed-release key, is stored within secure cloud storage. When a user tries to access it, the following sequence is executed:

1) The AI-driven access control module approves the permit.
2) The time condition is checked for validation.
3) If validated, then the decryption key will be provided to them.

That makes for a very sound, intelligent twin-layer enforcement: in one layer authorization based on intelligence and another accountability through enforcement that ensures high levels not only of confidentiality but also integrity.

3.8. Security advantages of the proposed framework

The proposed framework provides security improvements over existing approaches in the following aspects [1]:

a. AI-intelligent behavioral analytics detect and prevent insider misuse.
b. Timed-release encryption prevents access to data before its intended release time.
c. Attribute-based policies enforce fine-grained access control restrictions.
d. The system remains resilient to data breach attempts and compromise activities.

This makes a very strong yet flexible security solution for today's telecom data landscape when an AI intelligence layer is added on top of enforced cryptography, as shown in Figure 3.

Sensitive information can be safeguarded using encryption techniques to boost privacy and trust that it is being transmitted securely. Researchers have created a variety of algorithms to address privacy and data security issues for telecom users. AI and encryption methods evaluate data using shared infrastructure resources to provide a higher level of service with less upkeep and management. Any data that are being carried must be shielded against privacy breaches and illegal access. There are several architectural approaches to controlling this transfer, but they all leave the data vulnerable to easy deciphering by an attacker. Since data are sent from local servers to the cloud computing platform over the Internet and often across cloud computing resources, encryption is essential in the telecom industry. Since all of this data transfer occurs over the Internet, sending data in plaintext poses a serious security and privacy risk. There are several methods for this data to be intercepted across networks; thus, extra security measures are required. This issue is mostly resolved by encryption, which ensures that the data cannot be decrypted while being sent. Data are transformed into a format that can only be decoded by those who possess the necessary keys or other access controls through the use of encryption [16]. Encrypted data are frequently called ciphertext, whereas decrypted data are just text. Symmetric, public-key, and asymmetric encryption, often known as private-key encryption, are the three main types of encryptions. In contrast to symmetric key encryption, which uses the same key for both encryption and decryption, asymmetric encryption creates a pair of keys, the public key of which encrypts the data and the private key decrypts it. Figure 4 shows the general types of encryption techniques.

Figure 4 depicts the recommended two-round data encryption technique. To ensure that the data cannot be decoded during transmission, the first round encrypts it. Data are transformed into a format that can only be interpreted by those with the necessary keys or other access controls through the use of encryption. Ciphertext is the term for encrypted data, whereas plaintext is the term for unencrypted data. The second phase employs AI in combination with the IDTRE algorithm to ensure that data cannot be understood by someone who obtains access to the telecom site's database. The objective of IDTRE is to "send a message into the future." Encrypting a communication to prevent the recipient from decoding the ciphertext until later is one method to do this. Such a primitive might be used, for example, to prevent an unscrupulous auctioneer from placing bids earlier in a sealed-bid auction, to prevent early electronic voting systems, and to delay the verification of a signed document in communication sites and situations. Since data breaches are still one of the biggest risks to customer safety and business continuity, data security affects both the company and the customer, irrespective of the industry. Being open and honest about the methods used to obtain data is, therefore, crucial to preserving loyalty and confidence [5]. Customers know that telecom companies gather information to bill them. If consumers wish to maintain control over their personal information, these businesses will need to provide them with explicit privacy rules as these techniques get more complex. To increase security, optimize operations, and customize user experiences, telecommunications networks include AI technology [13]. Some personal information is gathered in the telecom sector without

Figure 3
Two-stage security architecture combining conventional file encryption with an AI-driven decision layer (IDTRE)

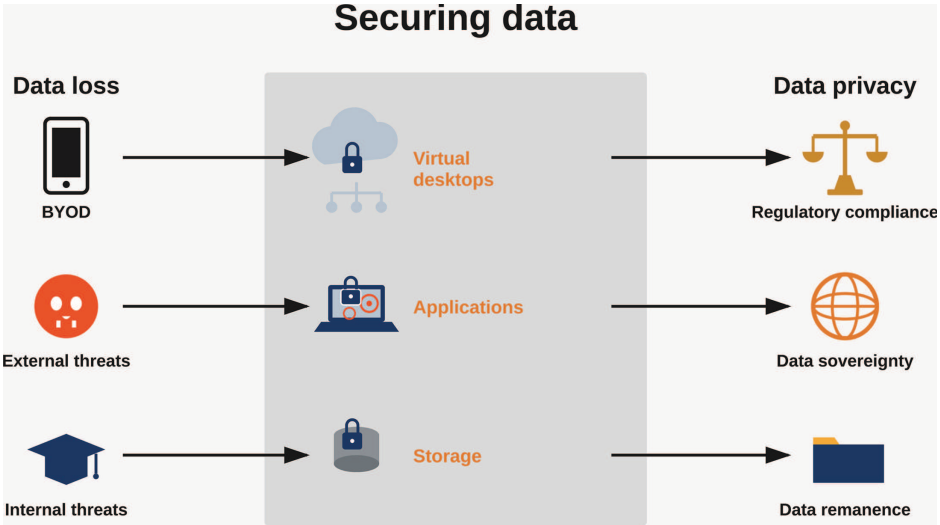
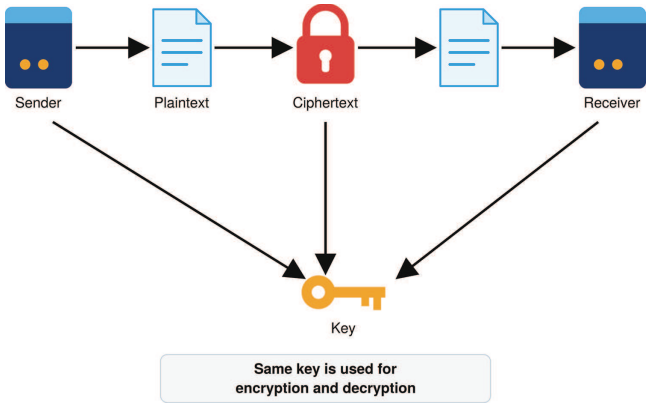


Figure 4
General data key encryption



our knowledge or consent. Localization, mobile devices, Internet connections, and online behaviors like website surfing and keyword entering into search engines all leave traces. For a variety of purposes, they can be observed and recorded. Predictive maintenance, network optimization, and intelligent customer service solutions are made possible by these technologies, which eventually increase productivity and please customers. As shown in Figure 5, the sender encrypts the file, and the same key is used to decrypt it upon receipt.

The AI-based access control module detects insider threats or misuse through behavior analysis. Fine-grained authorization policies are enforced using ABE, while timed-release encryption also enforces a policy by preventing any access before the allowed time; this integration ensures legitimate users get access within defined temporal constraints.

3.9. Algorithmic logic of the AI-IDTRE framework

The framework runs through a set of composite logical sequences to firmly enforce the proposed security layers. The access decision integrates both a behavioral classifier and a temporal validator.

Let:

a) $V = \{v_1, v_2, \ldots, v_n\}$ denote the behavioral and contextual feature vector extracted from an access request.
b) $R(V)$ denote the output of the trained Random Forest classifier.

The authorization function is defined as:

$$R(v) = \begin{cases} 1, & \textit{if the access request is classified as legitimate} \\ 0, & \textit{if the acess requesr is classified as malicious} \end{cases} \tag{4}$$

where

$$R(V) \in \{0, 1\} \tag{5}$$

Access Decision:

Let V be an input feature vector representing user behavior, such as the frequency of requests made by that particular user/location/role. Random Forest classifier R generates a probability score $P(v)$. The AI-based access decision (D_{AI}) can then be defined as follows:

$$D_{AI} = \begin{cases} 1, & if\ P\ (V)\ >\ T \\ 0, & otherwise \end{cases} \tag{6}$$

The access control logic is formally defined as a joint evaluation between behavioral authorization and temporal validation. The AI-based access module analyzes the behavioral feature vector of an access request, classifies it using a trained Random Forest model, and returns either legitimate or malicious authorization. This is further constrained by a time-based condition enforced through the timed-release encryption mechanism. Data access will only be granted if the request is both behaviorally authorized and temporally valid; otherwise, denial of access. The formal decision rule governing this process can be represented as follows:

$$D\ A1 = \begin{cases} Allow, & if\ R(V) = 1\ \wedge\ CurrentTime\ \geq\ T \\ Deny, & otherwise \end{cases} \tag{7}$$

Structured Pseudocode:

Algorithm 1: Behavior-Aware Time-Locked Access Control

Input: Access request r, user features V, release time T
Output: Plaintext data D or Access Denied
1) Extract behavioral and contextual features V
2) Compute $R(V)$ using the Random Forest model
3) If $R(V)$ == Deny then
4) Reject access request
5) Else
6) Check if CurrentTime $\geq T$
7) If time conditions are satisfied then
8) Release decryption key K
9) Decrypt data D
10) Else
11) Deny access (time constraint not met)
12) End if

4. Experimental Setup

This section specifies the experimental setup used in validating the efficiency of the proposed AI-IDTRE framework over a practical telecom data scenario.

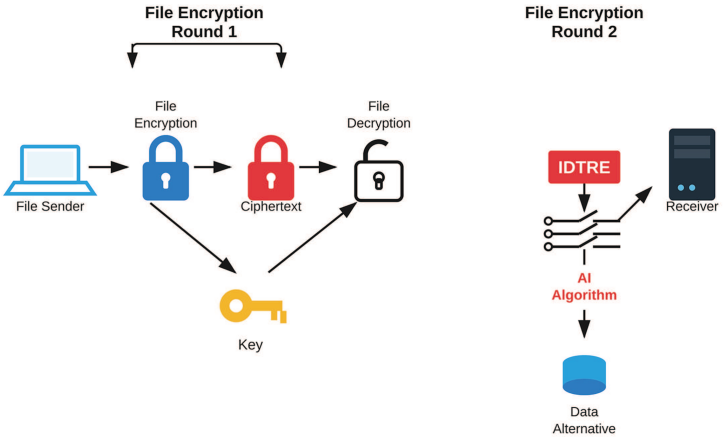
In this study, we used the IBM Telco Customer Churn dataset as a proxy dataset to emulate customer behavioral patterns for the AI-based access decision module. Though the dataset was primarily meant for churn prediction and marketing analysis, we leveraged several behavioral and service-related attributes to model patterns of access-and-access-under-control experimental conditions. These attributes serve as very good indicators for testing the decision-making capability of the AI-assisted framework being proposed.

But this dataset doesn't have cybersecurity-specific telemetry things like IP addresses, login timestamps, failed authentication attempts, or packet-level network features. So, the way it's set up now, this should be seen as a proof-of-concept evaluation rather than a full cybersecurity deployment.

4.1. Dataset description

We carried out experiments with the IBM Telco Customer Churn dataset. The IBM Telco Customer Churn dataset includes 7,043 customer records and 21 telephone-related attributes, such as customer tenure, service subscriptions, billing information, payment type, contract type, customer account characteristics, etc. The data were developed originally for predicting customer

Figure 5
The proposed method of encryption



churn; however, this study uses the data to model behaviorally access-controlled scenarios within telecom markets.

Many of the attributes present in the datasets used here convey some measure of behavior or context that is also considered when making decisions on access control. For example, attributes such as contract types, usage patterns of contract services, length of time as a customer, account activity, payment behavior, and profile information can all be viewed as contextual indicators of expected versus unexpected access activity.

4.2. Dataset adaptation for access control evaluation

Because the original IBM Telco Customer Churn dataset lacks access control labels, a behavioral access control simulation process was created to produce authorization classes for use in evaluating the AI-IDTRE framework. Contextual features representing customer activity patterns, such as tenure, monthly charges, total charges, service subscriptions, payment method, and contract type, were first selected as potential candidates for inclusion as contextual features to model user behavior. A rule-based labeling technique was then used to simulate both approved and unapproved access behavior, as aggregated records with logically consistent behavioral patterns were labeled as approved, while those with no relation to prior records indicating access were labeled as unapproved. Examples of simulated unapproved access behaviors are services being used inappropriately, inconsistent account characteristics, suspicious combinations of billing and subscription characteristics, and variance of customer behavior from the norm for all customers. Therefore, the dataset was changed into a binary (authorization vs. unauthorized) access control classification situation, which enabled a complete evaluation of the AI-based authorization component of the developed framework.

4.3. Data preprocessing

The following steps were applied to ensure the quality and consistency of the data:

a. Removal of records with missing or inconsistent values
b. One-hot encoding of categorical attributes
c. Min–max normalization of numerical features
d. Feature selection to eliminate redundant attributes

The dataset was split into 70% training data and 30% testing data for use in evaluating generalization.

4.4. AI model configuration

The Random Forest classifier was used as an AI-based access control model. This made the option of using a mixed type of data very easy, increasing robustness in the detection of anomalous behavior, because Random Forest happens to be one of the most robust classifiers [9].

Parameters were set for the model as follows:

a. Number of trees = 100
b. Splitting criterion = Gini Index
c. Maximum depth = determined automatically

The Random Forest model was trained using the labeled training data, which represented simulated legitimate and unauthorized access patterns. Through this training process, the model learned to distinguish between legitimate and suspicious access requests.

4.5. Baseline methods

The following baseline security mechanisms were considered in comparison with the proposed AI-IDTRE framework:

a. AES-256 encryption
b. ABE
c. AES combined with traditional role-based access control
d. These are among the most common telecom security approaches.

4.6. Experimental environment

All experiments and tests ran under exactly the same conditions to ensure fairness:

a. Processor: Intel Core i7
b. RAM: 16 GB
c. Operating System: Ubuntu 22.04
d. Programming Language: Python 3.10

Each experiment was repeated 10 times, and the average values are reported.

5. Evaluation Metrics

The following metrics were used for a holistic assessment of security and performance:

Security metrics

a. Access Accuracy (%): Ratio of correctly authorized access requests
b. Unauthorized Access Rate (%): Percentage of rejected malicious attempts
c. False Access Detection Rate (%): Incorrectly classified legitimate requests

Performance metrics

a. Encryption Time (ms)
b. Decryption Time (ms)
c. Computational Overhead (%)

AI Performance Metrics

a. Precision
b. Recall
c. F1-score

These metrics, in totality, comment on the confidentiality, efficiency, and intelligence of the proposed framework.

Standard classification metrics have been used in order to quantitatively evaluate the performance of an AI-based access control module. They include precision, recall, and F1-score. They are defined as follows:

$$Precision = \frac{TP}{TP + FP} \tag{8}$$

$$Recall = \frac{TP}{TP + FN} \tag{9}$$

$$F1 = x2\ \frac{Precision\ .\ Recall}{Precision + Recall} \tag{10}$$

6. Result

Results show that the proposed AI-IDTRE framework overwhelmingly outperforms traditional security mechanisms in all metrics evaluated. As also summarized in Table 2 and depicted by Figure 2, this method registers a maximum access control accuracy of 94.8% ± 1.1, which is quite higher relative to AES-256 at 82.4% ± 2.3, ABE being implemented at 86.7% ± 1.9 together with AES traditional access control at88 .1 % ± 1.6 This clearly demonstrates how effective ML-based decision-making can be when integrated into an access control process so that it dynamically distinguishes between legitimate and unauthorized attempts for system accesses.

In terms of security, the unauthorized access rate with AI-IDTRE drops to 5.2% ± 1.1, a little more than one-third of the rate recorded by its nearest baseline method, and this clearly reflects the potency of the proposed framework in thwarting external attacks and insider misuse through intelligent enforcement of authorizations and time-based restrictions. Although these components introduce additional computational overhead, they provide significant security benefits by strengthening behavioral authorization and enforcing time-based access restrictions.

The F1-score achieved by the AI-based access control module in abnormal access behavior detection stands at 94.6%. This, therefore, proves to be very reliable and confirms the robustness of classification performance for this model. A statistical paired t-test analysis of the results' significance proved that improvements were not just random variations since the result showed significance at a confidence level of less than 0.01 probability ($p < 0.01$). Therefore, experimental results validate an optimum trade-off found between enhanced security and computational overheads inside the proposed AI-IDTRE framework, making it a practical yet efficient solution toward securing sensitive telecom customer data. Table 1 gives a rundown of how the proposed AI-IDTRE framework stacks up against some baseline methods.

Table 3 reports the values for precision, recall, and F1-score of the AI-based access control module. These metric results present how well the proposed model has been able to classify rightful access as either anomalous or unauthorized access.

Table 3
AI-based access control performance

Model	F1-score	Recall	Precision
Traditional Access Control	85.0	83.7	86.3
AI-IDTRE (Random Forest)	94.6	94.2	95.1

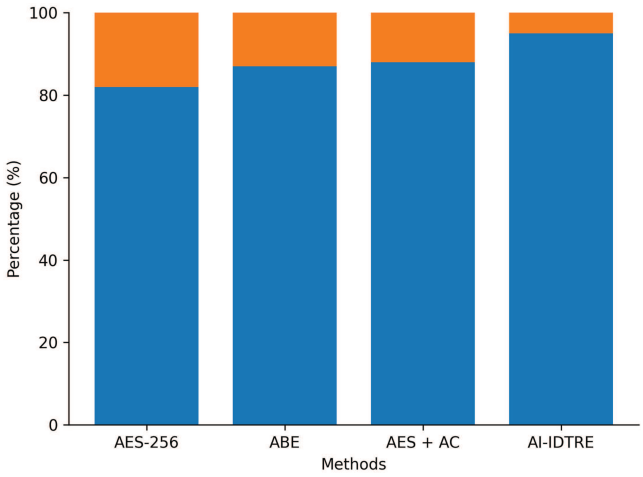
To highlight the difference in performance between the tested security mechanisms, a visual comparison of their effectiveness in access control has been provided. Figure 5 shows a comparison between the proposed AI-IDTRE framework and baseline encryption methods in terms of access accuracy and unauthorized access rate. It substantially reflects the effect of intelligent access control together with timed-release encryption on making the system holistically secure. The comparison of access accuracy and unauthorized access across different security methods is shown in Figure 6.

Figure 5 presents a visual comparison between baseline encryption methods and the proposed AI-IDTRE framework. The proposed approach achieves maximum access accuracy with minimum unauthorized access attempts; in other words, this result clearly demonstrates the effect of an AI-based access control sys-

Table 2
Gives a rundown of how the proposed AI-IDTRE framework stacks up against some baseline methods

Method	Encryption time (ms)	Decryption time (ms)	Unauthorized access rate (%)	Access accuracy (%)
AES-256	14.2 ± 1.1	13.7 ± 1.0	17.6 ± 2.3	82.4 ± 2.3
ABE	21.9 ± 1.6	20.8 ± 1.4	13.3 ± 1.9	86.7 ± 1.9
Proposed AI-IDTRE	24.6 ± 1.8	23.4 ± 1.6	5.2 ± 1.1	94.8 ± 1.1
AES + traditional Access Control	18.5 ± 1.3	17.9 ± 1.2	11.9 ± 1.6	88.1 ± 1.6

Figure 6
Access accuracy and unauthorized access comparison for different security methods



tem combined with timed-release encryption to improve telecom data security without massive degradation in performance.

6.1. Statistical analysis

A paired t-test was performed between the proposed framework and each baseline. The results show improvements in access accuracy and reduction of unauthorized access that are statistically significant with $p < 0.01$, thus firmly establishing the robustness of the proposed method.

6.2. Comparison with recent AI-driven security frameworks

Zero Trust AI security and behavior-aware authorization models [17–19], primarily based on inference of behavior or policy decisions, allow access but do not enforce any form of cryptographic time locking. The proposed AI-IDTRE is the first system to integrate both timed-release encryption and an actual AI-based access control component that would prevent premature disclosure even by authorized users. Table 3 shows the comparison between recent frameworks in AI-driven security and the proposed framework.

Table 4 illustrates the trend within current security frameworks of focusing primarily on intelligent behavioral analysis OR cryptographic protection—although not together (e.g., Zero Trust architectures utilize context-aware authorization and behavior verification; however, they do not implement cryptographic time-based access restrictions; AI-based intrusive detection systems in conjunction with encryption can enhance an organization's ability to detect attacks; however, they do not provide any temporal controls for data disclosure) [20–22]. Similarly, ABE allows fine-grained access control, while Timed-Release Encryption allows delayed decryption; however, they do not make use of adaptive AI-driven behavioral authorization [23, 24]. Therefore, the proposed AI-IDTRE framework will consolidate all of these capabilities into a single unified telecom-oriented architecture to allow for simultaneous intelligent authorization, mitigation of insider threats, cryptographic protection, and time-controlled enforcement of access [25–31].

7. Discussion

The experimental results justify the fact that an AI-based approach with timed-release encryption makes telecom data security much stronger than the normal encryption-based approaches. It has been observed that the AI-IDTRE framework attains better access control accuracy with a highly minimal rate of unauthorized access and, hence, effectively addresses both external attacks and insider threats. The proposed AI-based access control module dynamically evaluates access behavior to complement an approach based on static credentials or policies so that usage patterns can be captured automatically by the system and any anomalous activity is reliably detected.

What this clearly brings out is that intelligent decision-making has to be integrated with encryption for results such as these: timed-release encryption does not allow access before the due time, even for an authorized user within a window of temporal allowance outside which sensitive information cannot be decrypted. Telecom environments embody constraints on customer data from regulation, auditing, and operation across several parallel dimensions, where this capability becomes highly relevant. The framework thus overlays another layer stronger

Table 4
A comparative analysis between the proposed framework and recent frameworks in AI-driven security (2024–2025)

Framework	AI-based	Time-locked	Cryptographic enforcement	Telecom-oriented	Context-aware authorization	Insider threat detection
Zero Trust	√	x	x	x	√	√
AI-based Intrusion Detection System (IDS) + Encryption	√	x	√	x	Limited	√
Attribute-Based Encryption (ABE) Systems	x	x	√	x	√	x
Timed-Release Encryption	x	√	√	x	x	x
AI-IDTRE (Proposed)	√	√	√	√	√	√

than policy-based access control by applying time-based restriction at a lower cryptographic level. The proposed framework does add computational overhead in terms of AI processing and timed key management; however, results show that it stays well within practical limits for real-world implementation. A slight increase noticed in encryption and decryption time can be very well compensated for by the massive improvements found regarding security and accuracy of access. Random Forest permits quick inference, making this framework applicable to large-scale telecom systems. Results clearly state that the proposed AI-IDTRE framework has a balanced trade-off between enhanced security and system performance, thereby bringing out an actual pragmatic scalable solution suitable for protecting sensitive telecom customer data across modern network environments. The observed encryption overhead is about 10 MS per record, which is quite acceptable for small-scale experiments. But telecom systems work at much larger scales and with high concurrency requirements. In large deployments, we can use performance optimization techniques such as batch encryption, distributed processing, parallel execution, and hardware acceleration to minimize the latency bottlenecks. Scalability evaluation in real telecom environments remains a part of future work.

8. Limitation

The proposed AI-IDTRE framework has been proven effective. However, it also leaves certain limitations that can be considered aspects for potential future work and improvements. First is the extra computational overhead brought about by the integration of AI-based access control together with timed-release encryption in this framework. The overhead remains within acceptable limits based on experiments conducted but may need further optimization to ensure low latency under maximum load conditions in large-scale telecom deployments where high-frequency access requests are made.

Second, the framework depends on accurate and consistent attribute management for effective encryption and access control. Attributes include user roles, contextual information such as location or device, and logs of access requests. If any attributes are inaccurate or outdated, this could be manifested in wrong contextual details about a user's location high up in an organization; the result will be incorrect access decisions by the system or delays in making data available to legitimate users. High-quality attributes dynamically generated within telecom environments remain difficult to achieve plus they may necessitate extra administrative and system-level controls.

Third, it creates a certain level of rigidity in its operations. While timed-release encryption strictly enforces security by denying access to information before the appropriate time, legitimate users may also be subjected to delays if time parameters are not carefully set. This is mostly applicable in real or urgent operational contexts where data needs to be accessed immediately; hence, another adaptive time management strategy could address this issue. Finally, at present, the framework has been evaluated in a centralized cloud-based setting. This is again applicable to several telco use cases but may have potential scalability challenges in massively distributed or edge-based environments. The AI model may need retraining or reconfiguration to adapt to heterogeneous infrastructure and changing access patterns. These limitations drive enhancements in future releases toward a more scalable, flexible, and real-time responsive solution.

9. Conclusion

This paper proposed a very wide AI-IDTRE framework to secure by integrating ML intelligent access control with ABE and timed-release key management and telecom customer data in addressing critical shortcomings of traditional security mechanisms related mainly to insider misuse and premature access to data. Besides contextual authorization, this composite security framework enforces both authorization constraints and temporal constraints at the cryptographic level, hence suited adaptively for modern telecom environments. Results prove, with real data from the telecom domain, that this framework improves the accuracy of access control while reducing a large number of unauthorized attempts at access. The improvements are statistically significant as per the analysis of results, thus validating and confirming the effectiveness and reliability of this proposed approach. This solution/framework comes with moderate computational overhead but importantly here is that security benefits have been proven to outweigh associated performance costs hence making it viable or practical enough for actual deployment/use in real life.

Experimental results achieve 94.8% accuracy, conducted on a large-scale telecom dataset, in distinguishing between authorized and unauthorized access requests. AI-driven gates have an average latency overhead of about 10.4 ms. The trade-off is totally justified by the extreme reduction of attempts for gaining unauthorized access, together with an enhancement in data privacy via time-locked decryption. A statistical validation ($p < 0.05$) strongly supports the conclusion that the AI-IDTRE framework is far more effective than the conventional AES-256 and standard ABE models in the proactive mitigation of threats, thereby laying an inference on record for future reference, where further research shall involve fine-tuning the Random Forest inference engine to suit a real-time edge computing environment besides experimenting with federated learning integration aimed at enhancing privacy-preserving model updates across distributed telecom nodes.

Using the IBM Telco Customer Churn dataset provides one limitation of this work, as it is not designed explicitly for cybersecurity applications. It comes with very informative behavioral indicators but does not contain access logs and network telemetry of a security-specific nature. Future work will validate the proposed framework using dedicated cybersecurity datasets such as CICIDS and UNSW-NB15 or real telecom security logs to enhance realism and robustness.

Future work will focus on a federated, edge-based AI model to support distributed telco architectures for scalability and flexibility. It is also planned to make the time-release mechanism more adaptive besides further optimizing lightweight cryptography for lower latencies and better responsiveness in time-critical applications. Proposed AI-IDTRE is an advanced evolution of frameworks that ensure sensitive telecom customer data with increasing complexities and intelligence within network environments.

Acknowledgment

The authors gratefully acknowledge Universiti Tenaga Nasional (UNITEN) for financial support through the UNITEN Publication Fund. They also sincerely thank the reviewers for their valuable comments and suggestions, which helped improve the quality of this manuscript.

Funding Support

This research was supported by the UNITEN Publication & Conference Support Fund 2026 and supported by Institute of Information & Computing in Energy and Centre of AI Application & Innovation, College of Computing & Informatics UNITEN.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Waleed A. Hammood: Conceptualization, Validation, Writing – original draft, Writing – review & editing, Project administration. **Noor Akma Abu Bakar:** Writing – review & editing, funding acquisition. **Salwana Mohamad Asmara:** Software, Data curation, Supervision. **Surizal Nazeri:** Writing – review & editing. **Ejiro U. Osiobe:** Methodology, Writing – original draft, Writing – review & editing, Project administration. **Omar Abdulmaged Hammood:** Formal analysis, Visualization. **Marshima Mohd Rosli:** Investigation. **Salah A. Aliesawi:** Software, Resources.

References

[1] Soori, M., Arezoo, B., & Dastres, R. (2023). Artificial intelligence, machine learning and deep learning in advanced robotics, a review. *Cognitive Robotics*, *3*, 54–70. https://doi.org/10.1016/j.cogr.2023.04.001

[2] Hammood, W. A., Hammood, O. A., Asmara, S. M., & Lah, M. S. C. (2025). Customer behavior analysis for forecasting customer attrition: An artificial intelligence approach. *International Journal on Advanced Science, Engineering and Information Technology*, *15*(3), 1–6. https://doi.org/10.18517/ijaseit.15.3.12816

[3] Chakrabarty, S., Deb, C. K., Marwaha, S., Haque, M. A., Kamil, D., Bheemanahalli, R., & Shashank, P. R. (2026). Application of artificial intelligence in insect pest identification–A review. *Artificial Intelligence in Agriculture*, *16*(1), 44–61. https://doi.org/10.1016/j.aiia.2025.06.005

[4] Hammood, W. A., Hammood, O. A., Aliesawi, S. A., Osiobe, E. U., Hasan, R. A., Malallah, S., & Abbas, D. H. (2024). Data analysis of an exploring the information systems success factors for early warning systems adoption. *Babylonian Journal of Machine Learning*, 102–111. https://doi.org/10.58496/BJML/2024/010 *2024*

[5] Saini, H., Singh, G., Dalal, S., Lilhore, U. K., Simaiya, S., & Dalal, S. (2024). Enhancing cloud network security with a trust-based service mechanism using k-anonymity and statistical machine learning approach. *Peer-to-Peer Networking and Applications*, *17*(6), 4084–4109. https://doi.org/10.1007/s12083-024-01759-y

[6] Haque, S. A., & Al Jufaili, S. M. (2026). Applications of artificial intelligence in fisheries: From data to decisions. *Big Data and Cognitive Computing*, *10*(1), 19. https://doi.org/10.3390/bdcc10010019

[7] Kalhori, S. R. N., Najafi, F., Hasannejadasl, H., & Heydari, S. (2025). Artificial intelligence-enabled obesity prediction: A systematic review of cohort data analysis. *International Journal of Medical Informatics*, *196*, 105804. https://doi.org/10.1016/j.ijmedinf.2025.105804

[8] Zhang, J., & Jiang, S. (2024). Review of artificial intelligence applications in construction management over the last five years. *Engineering, Construction and Architectural Management*, *3*(1), 361–379. https://doi.org/10.1108/ECAM-03-2024-0313

[9] Joshi, G., Jain, A., Araveeti, S. R., Adhikari, S., Garg, H., & Bhandari, M. (2024). FDA-approved artificial intelligence and machine learning (AI/ML)-enabled medical devices: An updated landscape. *Electronics*, *13*(3), 498. https://doi.org/10.3390/electronics13030498

[10] Wang, C., Li, T., Lu, Z., Wang, Z., Alballa, T., Alhabeeb, S. A., . . . , & Khalifa, H. A. E. W. (2025). Application of artificial intelligence for feature engineering in education sector and learning science. *Alexandria Engineering Journal*, *110*, 108–115. https://doi.org/10.1016/j.aej.2024.09.100

[11] Zhang, L., Li, Y., Pan, Y., & Ding, L. (2024). Advanced informatic technologies for intelligent construction: A review. *Engineering Applications of Artificial Intelligence*, *137*, 109104. https://doi.org/10.1016/j.engappai.2024.109104

[12] Ji, B., Zhang, M., Xing, L., Li, X., Li, C., Han, C., & Wen, H. (2023). Research on optimal intelligent routing algorithm for IoV with machine learning and smart contract. *Digital Communications and Networks*, *9*(1), 47–55. https://doi.org/10.1016/j.dcan.2022.06.012

[13] Manley, K., Nyelele, C., & Egoh, B. N. (2022). A review of machine learning and big data applications in addressing ecosystem service research gaps. *Ecosystem Services*, *57*, 101478. https://doi.org/10.1016/j.ecoser.2022.101478

[14] Liu, R., Ali, S., Bilal, S. F., Sakhawat, Z., Imran, A., Almuhaimeed, A., . . . , & Sun, G. (2022). An intelligent hybrid scheme for customer churn prediction integrating clustering and classification algorithms. *Applied Sciences*, *12*(18), 9355. https://doi.org/10.3390/app12189355

[15] El-Hajj, M. (2025). Enhancing communication networks in the new era with artificial intelligence: Techniques, applications, and future directions. *Network*, *5*(1), 1–45. https://doi.org/10.3390/network5010001

[16] Chen, M., & Meers, J. (2026). Timed commitments and timed encryption: generic constructions and instantiations from isogenies. In N. Heninger, & M. Rosulek (Eds.), Annual International Cryptology Conference (pp. 447-477). Springer. https://doi.org/10.1007/978-3-032-35398-6_15

[17] Shokouhifar, M., Fanian, F., Rafsanjani, M. K., Hosseinzadeh, M., & Mirjalili, S. (2024). AI-driven cluster-based routing protocols in WSNs: A survey of fuzzy heuristics, metaheuristics, and machine learning models. *Computer Science Review*, *54*, 100684. https://doi.org/10.1016/j.cosrev.2024.100684

[18] Fang, H., Xu, L., Nan, G., Zheng, D., Zhao, H., & Wang, X. (2025). Accountable distributed access control with privacy preservation for blockchain-enabled internet of things systems:

A zero-trust security scheme. *IEEE Internet of Things Journal*, *12*(11), 17936–17947. https://doi.org/10.1109/JIOT.2025.3540868

[19] Hammood, W. A. (2025). Investigating factors affecting AI adoption in higher education using structural equation modelling (SEM). *KHWARIZMIA*, 50–57. https://doi.org/10.70470/KHWARIZMIA/2025/006 *2025*

[20] Amiludin, N. A., Rosli, M. M., Ibrahim, N., & Hammood, W. A. (2025). Mental health prediction using ensemble learning approaches with rebalancing technique. In *2025 International Conference on Advanced Machine Learning and Data Science*, 455–460. https://doi.org/10.1109/AMLDS63918.2025.11159407

[21] Song, H. J., Shin, N., Koo, H. M., & Shin, W. S. (2025). The impact of functional and service quality on perceived security in manufacturing and telecommunication services. *International Journal of Quality & Reliability Management*, *42*(2), 504–526. https://doi.org/10.1108/IJQRM-07-2021-0218

[22] Imani, M., Joudaki, M., Beikmohammadi, A., & Arabnia, H. R. (2025). Customer churn prediction: A systematic review of recent advances, trends, and challenges in machine learning and deep learning. *Machine Learning and Knowledge Extraction*, *7*(3), 105. https://doi.org/10.3390/make7030105

[23] Yang, W., Acuto, A., Zhou, Y., & Wojtczak, D. (2026). A survey for deep reinforcement learning based network intrusion detection. *Applied AI Letters*, *7*(2), e70026. https://doi.org/10.1002/ail2.70026

[24] Bouzaachane, K., El Guarmah, E. M., Alnajim, A. M., & Khan, S. (2026). Automated intrusion detection system leveraging dynamic computational intelligence algorithms. In M. Azrour & A. Alabdulatif (Eds.), *AI-driven security for next-generation IoT systems* (pp. 39–56). Springer. https://doi.org/10.1007/978-3-032-08784-3_4

[25] Chen, H., You, G. R., & Shiue, Y. R. (2024). Hybrid intrusion detection system based on data resampling and deep learning. *International Journal of Advanced Computer Science and Applications*, *15*(2), 121. https://doi.org/10.14569/ijacsa.2024.0150214

[26] Salman, S. A., Dheyab, S. A., Salih, Q. M., & Hammood, W. A. (2023). Parallel machine learning algorithms. *Mesopotamian Journal of Big Data*, *3*(1), 12–15. https://doi.org/10.58496/MJBD/2023/002

[27] Rahim, R., & Chishti, M. A. (2025). IoT security innovations: Recent technologies, threats, and solutions. *SN Computer Science*, *6*(6), 593. https://doi.org/10.1007/s42979-025-04106-x

[28] Fakherldin, M. A. I., Adam, K., Bakar, N. A. A., & Majid, M. A. (2019). Weather data analysis using Hadoop: Applications and challenges. In *IOP Conference Series: Materials Science and Engineering*, *551*(1), 012044. https://doi.org/10.1088/1757-899X/551/1/012044

[29] Kabir, M. I., Abubakar, A., Bakar, N. A. A., Majid, M. A., & Rahman, A. (2026). Integrating ABM and GIS for flood evacuation planning: A systematic review and future direction. *International Journal of Advanced Computer Science and Applications*, *17*(2), 1–14. https://doi.org/10.14569/IJACSA.2026.0170221

[30] Jemat, A., Yussof, S., Sameon, S. S., Aris, H., Ghapar, A. A., & Nazeri, S. (2023). Energy efficiency improvement and strategies in Malaysian office buildings (tropical climate): A review. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *29*(2), 72–80. https://doi.org/10.37934/araset.29.2.7280

[31] Nursal, A. T., Omar, M. F., & Nawi, M. N. M. (2021). Text pre-processing for the frequently mentioned criteria from online community homebuyer dataset. *International Journal of Interactive Mobile Technologies*, *15*(6), 171–184. https://doi.org/10.3991/ijim.v15i06.20801

How to Cite: Hammood, W. A., Bakar, N. A. A., Asmara, S. M., Nazeri, S., Osiobe, E. U., Hammood, O. A., …, & Aliesawi, S. A. (2026). An AI-Assisted Timed-Release Encryption Framework for Enhancing Telecom Customer Data Security. *Artificial Intelligence and Applications*. https://doi.org/10.47852/bonviewAIA62029196