IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 27 January 2024, accepted 13 February 2024, date of publication 23 February 2024, date of current version 29 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3369604

RESEARCH ARTICLE

Improving Digital Forensic Security: A Secure Storage Model With Authentication and Optimal Key Generation Based Encryption

ABDULLAH MUJAWIB ALASHJAEE[1] AND FAHAD ALQAHTANI[2]
[1]Department of Computer Sciences, Faculty of Computing and Information Technology, Northern Border University, Rafha 91911, Saudi Arabia
[2]Department of Computer Science, Prince Sattam Bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia

Corresponding author: Abdullah Mujawib Alashjaee (abdullah.alashjaee@nbu.edu.sa)

ABSTRACT Secure storage model for digital forensics represents essential progress in the domain, addressing the major problems associated with protecting and maintaining digital evidence. This method employs recent encryption systems and optimal key generation methods to ensure the confidentiality and integrity of data throughout the investigative process. Cloud forensics is an intelligent development of digital forensics to be preserved against online hacking. But, centralized evidence gathered and preservation reduces the reliability of digital evidence. The architecture for digital forensics in an Infrastructure as a Service (IaaS) cloud platform is a crucial structure intended to simplify the collection and protection of evidence while preserving the integrity and origin of digital objects within cloud-based methods. This architecture integrates numerous modules and methods to address the exclusive tasks modeled by cloud computing (CC) environments in the framework of forensic investigations. This paper develops a new digital forensic architecture utilizing the Authentication with Optimal Key Generation Encryption (DFA-AOKGE) technique. The main intention of the DFA-AOKGE method is to use a BC-distributed design to allocate data between numerous peers for data collection and safe storage. Additionally, the DFA-AOKGE model uses the Secure Block Verification Mechanism (SBVM) for the authentication procedure. Also, the secret keys can be produced by the usage of the Enhanced Equilibrium Optimizer (EEO) model. Furthermore, the encryption of the data takes place using a multikey homomorphic encryption (MHE) approach and is then saved in the cloud server. The simulation value of the DFA-AOKGE methodology takes place in terms of different aspects. The simulation results exhibited that the DFA-AOKGE system shows prominent performance over other recent approaches in terms of different measures.

INDEX TERMS Key generation, encryption, decryption digital forensic architecture, multikey homomorphic encryption.

I. INTRODUCTION

An increase in cyberattacks and data exploitation has developed the requirement for leading digital analyses. Standardization and reliability for better performances have become crucial for providing the minimum number of human errors due to irrelevant evidence [1]. Forensic artifacts are the most significant once they derive analysis and process, as they offer evidence of an occurrence. While forensic artifacts exist in a judicial court, they are subject to inspection and need cross-examination and verification. Digital evidence is required to maintain the Confidentiality, Integrity, Availability (CIA) triad, such as accessibility, integrity, and confidentiality [2]. The confidentiality of digital evidence should be safeguarded due to the evidence can include sensitive data like credit card data and other individual identifiers.

The associate editor coordinating the review of this manuscript and approving it for publication was Shuangqing Wei.

To secure the evidence, severe access control is required or an encryption technique can be employed to make sure that only authorized parties or an investigator access the digital evidence [3]. Confirming the integrity of the digital evidence is a major significant procedure of some digital analysis, as an investigator is required to demonstrate that the evidence is not tampered with or fabricated in some way.

To accomplish this, a forensic copy of the original evidence, and chain of custody and software logs are maintained. The development succeeded the inspector in obtaining the evidence also desired as documented [4]. The forensic hash of the evidence requires to be considered numerous times – in the period of gathering and storage – to confirm that the original evidence could not altered, as well as the method accompanied by the investigator is wide-ranging and cannot change the evidence in some manner [5]. Consequently, a protective storage method can be desirable for enhancing the investigation way and protecting any sensitive data gathered. A similar issue affects digital forensic readiness models, either smaller and larger organizations or even specific persons. These methods gather effectively evidence, thus, storage processes and evidence protection can be important to confirm that evidence is authentic and valid [6].

Blockchain (BC)-based cloud forensics model provides an efficient performance for forecasting privacy leakage in cloud platforms. This method integrates the immutability and transparency of BC technology with the proficiencies of cloud forensics for improving security and privacy [7]. Cloud environments depend on a cloud platform but, information and services could be presented. It is a private cloud, public cloud, or hybrid cloud infrastructure. With respect to data collection, different information sources in the cloud platform have been gathered and monitored for investigation [8]. It comprises system activities, logs, user activities, network traffic, and other related data points. User authentication is a leading method of cloud forensics for safeguarding higher-level security. Now, the important goal is to protect evidence from unauthorized users [9]. Email verification and a one-time password (OTP) could be employed for efficient authentication. Possibly BC-assisted cloud forensic model has protected; it also has robust authentication that is needed for evidence sources [10].

This paper presents a novel digital forensic architecture using the Authentication with Optimal Key Generation Encryption (DFA-AOKGE) technique. The DFA-AOKGE model presents innovation over its new integration of a BC-distributed plan for decentralized data allocation and a multi-key homomorphic encryption technique, safeguarding safe and clear digital forensic procedures. The purpose of the DFA-AOKGE technique is to apply a BC-distributed architecture to distribute data among several peers for evidence collection and secure storage. In addition, the DFA-AOKGE technique applies the Secure Block Verification Mechanism (SBVM) for the authentication process. Besides, the secret keys can be generated by the use of the Enhanced Equilibrium Optimizer (EEO) algorithm. Furthermore, the encryption of the data takes place using a multikey homomorphic encryption (MHE) approach and is then saved in the cloud server. The developed method incorporates authentication and encryption synergistically to strengthen the safety of digital forensic data. Authentication devices safeguard that only official personnel with genuine credentials can entree the method, stopping illegal entry. Simultaneously, encryption defends the honesty and privacy of the kept data, making it strong for illegal tampering or access. The harmonious addition of authentication and encryption not only creates a strong defense besides potential safety breaches but also confirms a complete model for safe digital forensic data, improving the general honesty and privacy of critical data through the investigative procedure. The experimental validation of the DFA-AOKGE technique takes place in terms of different measures. The key contributions of the study are summarized as follows:

- Presents a new digital forensic design, DFA-AOKGE, which influences Authentication with Optimal Key Generation Encryption. This architecture signifies a forward-looking technique to improve the safety and efficacy of digital forensic procedures.
- Integrates a BC-distributed plan for data allocation between many peers. This contribution certifies decentralized data collection and safe storage, delivering enhanced flexibility and integrity to digital forensic data.
- Executes the SBVM as a fragment of the authentication process. This device improves the safety of the method by delivering a strong means of confirming the reality of data, ensuring the integrity of digital forensic proof.
- Presents the usage of the EEO technique for secret key generation. This contribution improves the cryptographic power of the system, providing a safe and effective model for producing secret keys vital for encryption and data safety.
- Uses a multi-key homomorphic encryption technique for data encryption earlier storage in the cloud server. This new encryption model safeguards protected and privacy-preserving computations, considerably donating to the confidentiality and defense of forensic data.

II. LITERATURE WORKS

Shankar et al. [11] developed a method dependent upon an asymmetric key cryptosystem and the client's biometric identifications. The Edwards-curve Digital Signature Algorithm (EdDSA), particularly Ed25519 was implemented to generate keys for document verification and signature. The EdDSA was employed with BC technology to indicate crypto wallets. The Python execution technique allows infrastructure self-reliance. In [12], an effective Identity-based cryptography (IBC) model was introduced to protect cloud storage, described as a Secure Cloud Storage System (SCSS) that assists encryption techniques and distributed key management as well as aids in numerous PKGs. In a

forensic investigation, the lawful authorities may be capable of employing several PKG methods for data availability, whereas an account locking approach avoids a single authority for accessing user information because of reliance distribution. Sheeja [13] projected the Multifactor Scalable Lightweight Cryptography for the Internet of Things (IoT)-Cloud. Encryptions for private and public cloud information could be achieved by the Digital Signature Algorithm (DSA) and Policy assisted Attribute encryption method with Moth fly optimizer (MFO). The optimizer was effectively selected as the key parameter. 3 multifactors can be further utilized for implementing 3 authentication levels via a trust-based Authentication technique.

In [14], the authors developed a BC-enabled digital forensics method for cloud computing platforms. In this method, the database was gathered and pre-processed by applying normalization. The pre-processed data have been stored in the BC network. The information is encoded and decoded as well as enhanced via a multi-objective krill herd cuckoo search optimizer algorithm (MKHCSOA). Deebak and Fadi [15] projected a lightweight smartcard-based secure authentication (LS-BSA) technique exploiting the mathematical rules. Further, this developed LS-BSA employs lightweight operations for accomplishing consistent data connectivity in a protected network. Formal security verification of BAN logic was presented to exhibit that LS-BSA provides appropriate secret secure-session key agreement and cooperative user authentication. Rajashree et al. [16] presented an architecture dependent upon the secure hash algorithm (SHA) algorithms and advanced encryption standard (AES) algorithmic protocol. SHA must be concurrently implemented as the AES method. Both receiver and transmitter units can be comprised in this architecture for securely transmitting and receiving information. This was designed by Xilinx ISE14.2, therefore the parameters of this developed algorithmic protocol were compared to several diverse Field-Programmable Gate Arrays (FPGAs) and compared factors with data encryption standard (DES) approaches resulting in acceptable outcomes.

In [17], a biometric authentication technique was developed. A cryptographic algorithm has been employed by service providers to create the bio-key for authentication. This introduced approach was contrasted to present techniques like randomized convergent encryption (RCE), secure de-duplication scheme (SDS), convergent encryption (CE), and leakage resilient (LR) for determination of the de-duplication efficiency. Henge et al. [18] designed a user-storage-transit-server authentication procedure framework dependent upon a mathematical post-quantum cryptography algorithm and protected key data distribution. The post-quantum cryptography mathematical model was exploited. It could be determined and comprised of the mathematical model for producing the allocated security key and data with on-editing, transit, and on-storage.

Liu et al. [19] present a novel Privacy-Preserving Reputation Updating (PPRU) method for cloud-assisted vehicular networks depends on the Elliptic Curve Cryptography (ECC) and Paillier algorithms, but the reputation feedback can be gathered and pre-processed by the honest but curious Cloud Service Provider (CSP) in a privacy-preserving system. Guo et al. [20] examine a trust assessment method for federated learning in Digital Twin for Mobile Networks (DTMN) that takes direct trust evidence and suggested trust data into account. A user behavior system can be designed to rely on several attributes to represent users' behavior in a fine-grained method. In [21], depends on improved Asymmetric Scalar-Product-Preserving Encryption (ASPE) intended in our conference version, the authors present a basic Privacy-preserving Spatial Data Query (PSDQ) approach by employing a novel unified index design that only needs users to offer lesser data about query range.

Though several techniques exist in the literature, it is still required to enhance safety performance. The present study in digital forensic image safety presently faces crucial gaps that require advanced solutions to address developing tasks. One prominent gap lies in the essential for a strong and clear decentralized framework, and BC technology presents a promising avenue. Integrating BC into digital forensic image safety can improve the reliability of the evidence chain, safeguarding traceability and immutability, thereby modifying the danger of tampering or illegal changes. Also, the present gap in safe cryptographic key generation models can be connected by discovering metaheuristic-based techniques. These models leverage optimizer models enthused by normal phenomena to produce cryptographic keys, offering improved safety over enlarged randomness and unpredictability. Moreover, there is a pressing requirement for innovative authentication devices to bolster access control in digital forensic states. Integrating multi-factor authentication and biometric confirmation can reinforce the complete refuge posture, certifying that only official personnel have entree to critical forensic image data. Addressing these gaps is vital for proceeding in the area of digital forensic image safety, fostering trust in the reliability of evidence, and reinforcing the resilience of investigative procedures in the face of developing cyber threats.

III. PROPOSED MODEL

In this section, the major problems including centralization of evidence gathering and protection, problems in integrity and security, and prohibited user access are sorted by centralization of evidence collection and preservation. The aforementioned problems are fixed and considered from the Cloud forensic architecture called Cloud DFA (CDFA). The software-defined networking (SDN) and BC technologies are used for analyzing and gathering evidence. The primary objective is to get reliable evidence in the Cloud platform and to keep data provenance for Cloud information. The entities such as CSP, SDN Controller, Authentication Servers, and Users of the Cloud are incorporated into the forensic system. Initially, it constructs a robust authentication system

to protect against unauthorized users. The data kept under the Cloud environment is encrypted to ensure security in the CSP according to the sensitivity level. The smart contract is used for tracing data history and for protecting data provenance. Fig. 1 illustrates the entire process of the DFA-AOKGE algorithm.

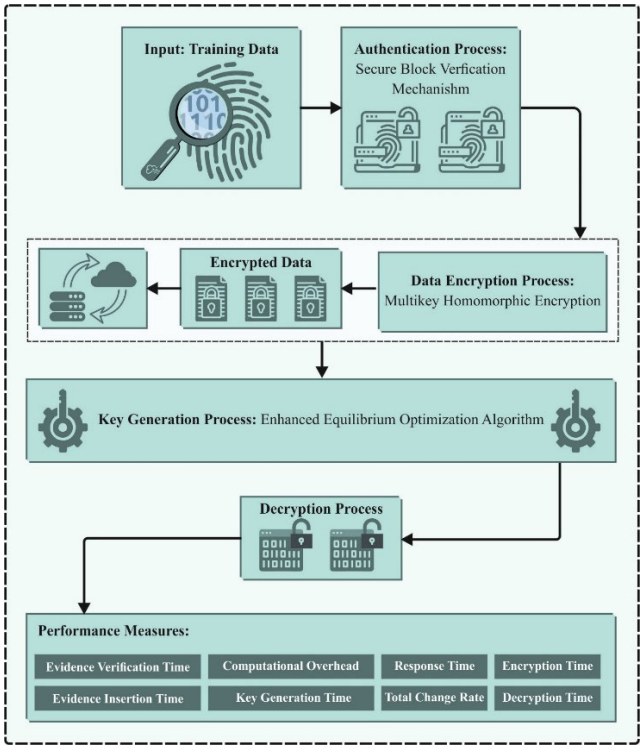


FIGURE 1. Overall process of the DFA-AOKGE algorithm.

A. USER AUTHENTICATION

Initially, each Cloud user registered with AS. During registration Password (PW), User ID (ID), and password are considered user credentials. AS makes use of the HSO method for producing a secret key (SK) for registered users (U). The PW, SK, ID, and Secret Code (SC) are circular theorems used for authenticating each user.

B. KEY GENERATION USING THE EEO ALGORITHM

The EEO algorithm can be used to generate the keys. The author introduced an EO based on the physics observations [22]. Especially, EO is derived from the physics law governing the balance of concentration of non-reactive constituents in a controlled volume. The below formula describes the mass conservation that enters and leaves a certain volume and the system often inclines to an equilibrium point. The initialization, equilibrium pool and candidate, and concentration upgrade are the three major steps of EO. Like MAs, initialization is dependent upon population growth, and EO randomly produces a population. The population includes particles and a uniform distribution was attained. Each particle is determined by the concentration vector. The initial population is produced from the following expression:

$$P_i^{initial} = P_{\min} + rand_i\,(P_{\max} - P_{\min})\; i = 1, 2, \ldots, n \quad (1)$$

In Eq. (1), the vector corresponding to the primary concentration of i^{th} particles is $P_i^{initial}$, and the upper and lower bounds are $P_{\max}$ and $P_{\min}$, correspondingly, the particle count in the population is n, and $rand_i$ is a random integer $\in [0, 1]$.

Equilibrium pool and candidate: EO applies a pool of five different particles to attain the unknown state of equilibrium, representing the optimum performance. The pool has four better particles for the diversification process. The average of 4 particles is applied for the exploitation purpose:

$$\vec{P}_{eq}, = \left[\vec{P}_{eq(1)}, \vec{P}_{eq(2)}, \vec{P}_{eq(3)}, \vec{P}_{eq(4)}, \vec{P}_{eq(avg)}\right] \quad (2)$$

Concentration upgrade: the EO is used to update the particle population at each iteration using the subsequent expression:

$$\vec{P} = \vec{P_{eq}} + \left(\vec{P} - \vec{P_{eq}}\right)\vec{F} + \frac{\vec{R}}{\vec{\lambda}}\left(1 - \vec{F}\right), \quad (3)$$

In Eq. (3), $\vec{F}$ influences the exploration and exploitation balance and is shown below:

$$\vec{F} = e^{-\vec{\lambda}(t-t_0)} \quad (4)$$

In Eq. (4), λ is a randomly generated number $\in [0, 1]$, and the value of t is reduced with an increased iteration counter,

$$t = \left(1 - \frac{iter}{\text{Max\_}iter}\right)^{\left(a_2\left(\frac{iter}{\text{Max\_}iter}\right)\right)} \quad (5)$$

In Eq. (5), $iter$ and Max$iter$ are the existing and the maximal iteration counter. The constant $a2$ is used to control the exploitation; as a_2 enhances, the intensification progresses, but the exploration ability reduces. The $\vec{t}_0$ vector is calculated by the following expression:

$$\vec{t}_0 = \frac{1}{\vec{\lambda}}\text{In}\left(-a_1 sign\,(\vec{r} - O.5)\left[1 - e^{-\vec{\lambda}t}\right]\right) + t, \quad (6)$$

In Eq. (6), the constant $a1$ is used to control the diversification. $sign(r-0.5)$ shows the intensification and diversification directions. The exploration capability rises with enhancing $a1$ values, however, the exploitation ability reduces. The $\vec{R}$ vector represents the generation rate and is calculated by the following expression:

$$\vec{R} = R\vec{C}P\left(\vec{P_{eq}} - \vec{\lambda}\vec{P}\right)e^{-\vec{\lambda}(t-t_0)} \quad (7)$$

where $R\vec{C}P$ is:

$$R\vec{C}P = \begin{cases} 0.5r_1 & r_2 > RP \\ 0 & otherwise, \end{cases} \quad (8)$$

Now, r_1 and r_2 are random integers $\in [0, 1]$, and the parameter RCP impacts the exploitation-exploration balance.

The EEO model incorporates the abovementioned approaches. Especially, the EEO used to initialize the population with LF distribution:

$$P_i^{initial} = P_{\min} + Levy\,(\beta) \times (P_{\max} - P_{\min}) \quad i = 1, 2, \ldots\ldots NP \tag{9}$$

In Eq. (9), the initial value of the i^{th} particle is $P_i^{initial}$, $and P_{\min}$ and $P_{\max}$ denote the low and up boundaries, correspondingly. Levy (β) is a levy flight (LF) random walking. Prior studies have demonstrated that LF enables powerful coverage of the searching space, and thus candidate performances are likely to converge toward the best solution. Prior work has proved that LF is a robust process for escaping regions with local minimum. Fig. 2 depicts the steps involved in EEO.

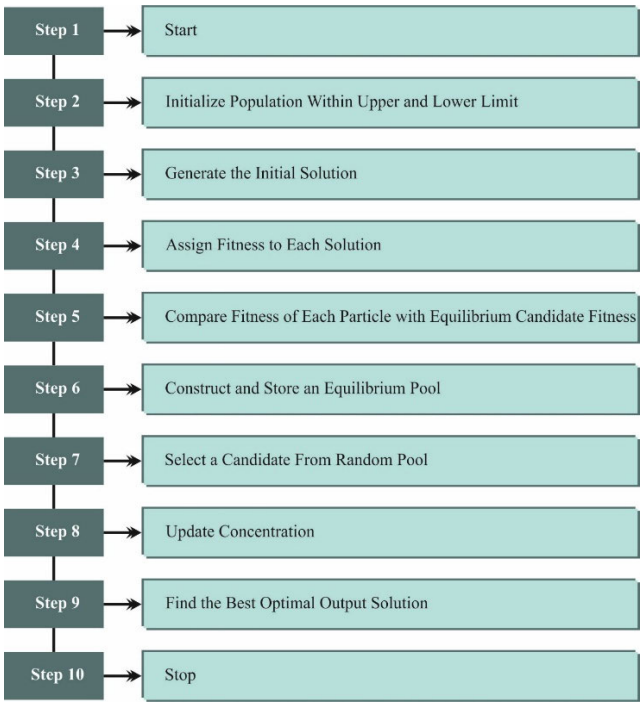


FIGURE 2. Steps involved in EEO.

Reinforce exploration: each particle widely searches the problem space from the exploration phase to detect potential areas. The exploration can be implemented by the original EO method including only searching nearby the optimum particles, viz., P_{eq}. Therefore, this study presents a novel reinforcement exploration technique that mutates the search particle by choosing 2 particles from the population:

1) According to the fitness values, the population is split into 2 different parts, viz., the optimum and worse performances;
2) The P_{r1} and P_{r2} solution from the optimum and worst fitness solutions is chosen by the tournament selection technique that can be described as follows:

$$Pt_j = Peq_j + \left(P_{r2}\,(j) - P_{i,j}\right) * x + \left(P_{i,j} - P_{r1}\,(j)\right) * y. \tag{10}$$

In Eq. (10), $thex, y$ operator retains the stochastic nature and defines the convergence way of searching particles, while producing Pt solution; x and y are randomly generated by the subsequent equation:

$$x = 0.05 + 0.95 * rand \tag{11}$$

$$y = 0.9 + 0.1 * rand \tag{12}$$

Here $rand$ is a randomly generated value within $\in [O, 1]$.

C. AUTHENTICATION PROCESS

Evidence and data are protected against malicious consumers by employing the SBVM [12] determined by a cloud authentication server (CAS). The SBVM contains consumers who have finished a positively safe verification procedure by means of a globular logic and secret key (SK).

CAS generates beginning points and secret keys for those logged-in users. The root point is (Ox, $and\ Oy$) coordinates for all the operators of specific circles [23]. The corresponding credentials (ID, PW, and SC) are protected for each user in CAS. All passwords are checked in each stage of verification. The CAS key is a random code being prevents the attacker from discovering the code for all the users. A circle is determined by the subsequent formula:

$$(Ax - Ox)^2 + (By - Oy)^2 = R^2 \tag{13}$$

All the users build an SC with an origin point(Ax, By). The user selects an SC which follows the circle equation to complete the validation. The user must have an ID and password together with the time stamp (TS) to use the cloud. The algorithm illustrates the SBVM-based authentication method. Users with legitimate passwords will effectively complete the authentication. The attacker cannot split the SC even though the SC varies over time. Notwithstanding the SC being cracked at a time by the attacker, they could not use SC for the next validation without knowing the source point.

D. ENCRYPTION USING THE MHE APPROACH

The MHE approach can be applied to the process of data encryption. MHE is a cryptosystem that enables to calculation of an arithmetic circuit on ciphertext, encrypt on various keys [24].

Consider M as a message space with arithmetic infrastructure. An MKHE system includes five probabilistic polynomial-time (PPT) algorithms
($Setup, KeyGen, Enc, Dec, Eval$). Given that, the participating party has an index (reference) to its secret and public keys. A multiple key ciphertext implicitly has a well-ordered set $T = \{id_1, \ldots, id_k\}$ of related reference. For instance, a new ciphertext $ct \leftarrow MKHE.Enc(\mu; pk_{id})$ is a single-element set $T = \{id\}$ however the size of the reference set becomes large as the computation between ciphertext in dissimilar parties develops.

- Setup: $pp \leftarrow MKHE.Setup(1^{\lambda})$. Take the security parameter as input and return the public parameterization. Consider that the other methods implicitly take pp as an input.

- Key Generation: $(sk, pk) \leftarrow MKHE.KeyGen(pp)$. Output a tuple of public and secret keys.
- Encryption: $ct \leftarrow MKHE.Enc(\mu; pk)$. Encrypt the plaintext $\mu \in M$ and output a ciphertext $ct \in \{0, 1\}^*$.
- Decryption: $\mu \leftarrow MKHE.Dec(\overline{ct}; \{sk_{id}\}_{id\in T})$. Assume a ciphertext $\overline{ct}$ with a similar series of secret keys, and output a plaintext μ.
- Homomorphic assessment:

$$\overline{ct} \leftarrow MKHE.Eval(, (\overline{ct}_1, \ldots, \overline{ct}_l), \{pk_{id}\}_{id\in T})$$

Consider a circuit C, a pair of multiple key ciphertexts $(\overline{ct}_1, \ldots, \overline{ct}_l)$, and the sequence of public keys $\{pk_{id}\}_{id\in T}$, output a ciphertext $\overline{ct}$. Its reference set is the union $T = T_1 \cup \cdots \cup T_l$ of reference sets T_j of the input ciphertexts $\overline{ct}_j$ for $1 \leq j \leq l$.

Semantic Security. For any 2 messages $\mu_0, \mu_1 \in M$, the distribution $\{MKHE.Enc(; pk)\}$ for $i = 0, 1$ must be equivalent where $pp \leftarrow MKHE.Setup(1^\lambda)$ and $(sk, pk) \leftarrow MKHE.KeyGen(pp)$.

Correctness and Compactness. An MKHE system is compact once the ciphertext size concerning k parties is limited by the poly (λ, k) for the fixed polynomial poly.

For $1 \leq j \leq \ell$, consider $\overline{ct}_j$ as a ciphertext (T_j) thus $MKHE.Dec(\overline{ct}_j, \{sk_{id}\}_{id\in T_j}) = \mu_j$. Where $C : M^l \rightarrow M$ is a circuit and $\overline{ct} \leftarrow MKHE.Eval(C, (\overline{ct}_1, \ldots, \overline{ct}_l), \{pk_{id}\}_{id\in T})$ for $T = T_1 \cup \cdots \cup T_l$.

$$MKHE.Dec(\overline{ct}, \{sk_{id}\}_{id\in T}) = C(, \ldots, \mu_l) \quad (14)$$

The equality of (14) is replaced by estimated equality comparable with the CKKS system for arithmetic operations.

E. BLOCKCHAIN-BASED EVIDENCE COLLECTION

Digital evidence is a major source for cybercrime investigations. The suspect may terminate the evidence and hide their information in the IaaS Cloud system location. The major issue is the sharing of data processing amongst computer resources. Furthermore, Cloud users have great control over the investigator, so collecting and maintaining evidence is a challenge. The CDFA used to leverage the SDN and BC technologies to gather and retain evidence from the Cloud to protect against those challenges. Evidence processing is crucial for accessing and categorizing forensic information from the cloud in the source and location. Evidence has been stored on a single physical host but information can spread over various regions. Consequently, it is difficult to locate proof after an incident. The proof is collected from different sources, such as random access memory (RAM) image files, hard drives, virtual machines, memory units, switches, hosts, routers, browsers, and servers. The information is collected from various sources. Evidence is gathered by information collected from memory space analysis, Cloud servers, and browser objects. In the presented DFA, SDN, and BC technologies are utilized to collect and keep forensic information to over these challenges. Evidence has been saved from the BC ledger on the control of SDN control.

IV. RESULT ANALYSIS AND DISCUSSION

In this section, the experimental result analysis of the DFA-AOKGE technique is extensively studied. In Table 1, a comprehensive comparison study of the DFA-AOKGE technique is provided [23]. In Fig. 3, a comparative response time (RT) results of the DFA-AOKGE technique is provided. The results show that the DFA-AOKGE system reaches enhanced performance with minimal RT values. With 10 users, the DFA-AOKGE technique offers decreased RT of 86.03ms whereas the FAuB and CFLOG models obtain increased RT values of 50.75ms and 78.68ms, respectively. Concurrently, based on 20 users, the DFA-AOKGE method offers a reduced RT of 88.96ms however, the FAuB and CFLOG algorithms get improved RT values of 52.22ms and 82.35ms, appropriately.

In Fig. 4, a comparison evidence insertion time (EIT) analysis of the DFA-AOKGE system is exhibited. The obtained outcome pointed out that the DFA-AOKGE model achieves enriched performance with decreased EIT values. Based on 10 users, the DFA-AOKGE technique gives a minimized EIT of 61.29ms while the FAuB and CFLOG algorithms get increased EIT values of 26.41ms and 48.11ms, individually. Also, with 20 users, the DFA-AOKGE methodology offers a diminished EIT of 62.84ms but, the FAuB and CFLOG algorithms get increased EIT values of 28.74ms and 50.44ms, correspondingly.

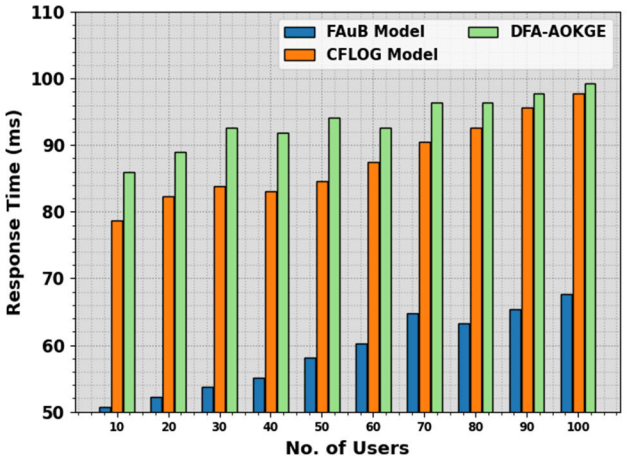


FIGURE 3. RT analysis of the DFA-AOKGE method under various users.

In Fig. 5, a comparison evidence verification time(EVT) analysis of the DFA-AOKGE method is determined. The attained outcome shows that the DFA-AOKGE model gains improved performance with reduced EVT values. According to 10 users, the DFA-AOKGE system gives a diminished EVT of 72.35ms while the FAuB and CFLOG algorithms get increased EVT values of 32.63ms and 58.87ms. Besides, with 20 users, the DFA-AOKGE methodology offers minimized EVT of 73.77ms but, the FAuB and CFLOG algorithms get increased EVT values of 36.18ms and 65.26ms, correspondingly.

TABLE 1. RT, EIT, and EVT outcome of DFA-AOKGE system with other approaches under various users.

No. of Users	FAuB Model	CFLOG Model	DFA-AOKGE
Response Time (ms)			
10	50.75	78.68	86.03
20	52.22	82.35	88.96
30	53.69	83.82	92.64
40	55.16	83.09	91.90
50	58.10	84.56	94.11
60	60.31	87.49	92.64
70	64.71	90.43	96.31
80	63.25	92.64	96.31
90	65.45	95.58	97.78
100	67.65	97.78	99.25
Evidence Insertion Time (ms)			
10	26.41	48.11	61.29
20	28.74	50.44	62.84
30	30.29	57.42	68.27
40	34.16	60.52	72.92
50	35.71	68.27	76.02
60	38.04	66.72	75.25
70	38.04	69.04	77.57
80	41.14	77.57	81.45
90	43.46	82.22	90.75
100	45.01	84.55	96.95
Evidence Verification Time (ms)			
10	32.63	58.87	72.35
20	36.18	65.26	73.77
30	38.31	61.71	73.06
40	40.43	67.39	73.06
50	40.43	70.93	79.44
60	46.11	68.10	80.15
70	42.56	71.64	84.41
80	43.27	69.51	83.70
90	46.82	75.19	87.96
100	47.53	78.03	89.37

Table 2 illustrates the comparative outcome of the DFA-AOKGE model with recent methods in terms of computational overhead (OC) and total change rate (TCR). The OC analysis of the DFA-AOKGE system with other models is evaluated in Fig. 6. The achieved outcome shows that the FAuB method gets poorer performance with decreased values of OC. Additionally, the CFLOG model acquires moderately booster OC values. However, the DFA-AOKGE methodology attains improved outcomes with increased values of OC with all users.

TCR results of the DFA-AOKGE technique with recent models are computed in Fig. 7. The results highlighted that

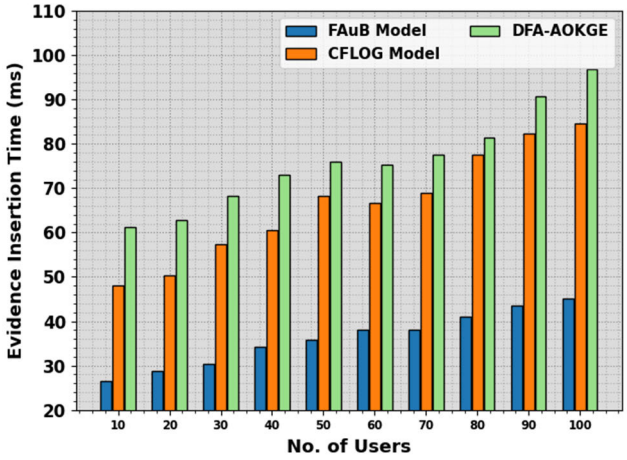


FIGURE 4. EIT analysis of the DFA-AOKGE algorithm under various users.

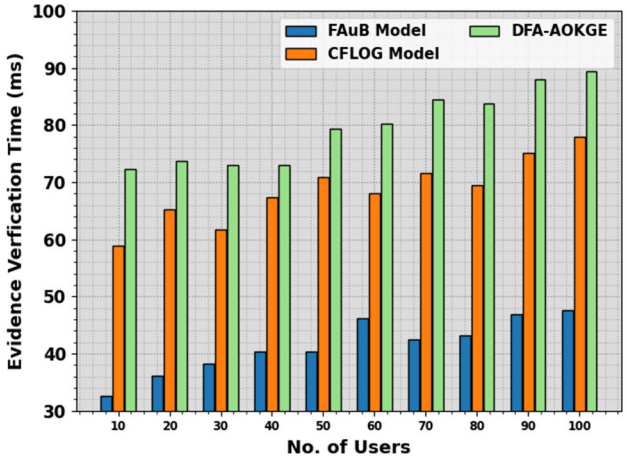


FIGURE 5. EVT analysis of the DFA-AOKGE model under various users.

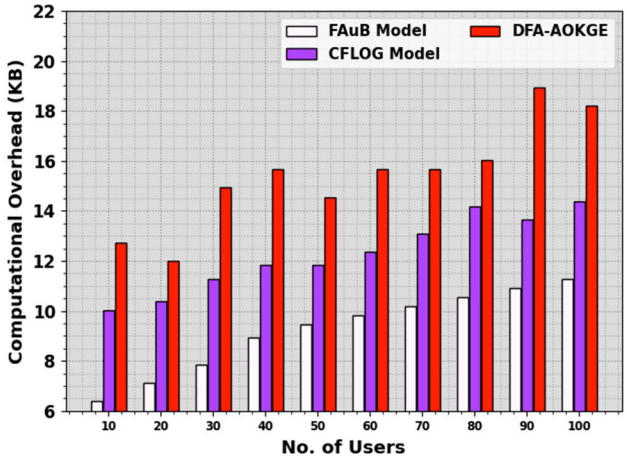


FIGURE 6. OC analysis of the DFA-AOKGE system under various users.

the FAuB model attains poor performance with reduced values of TCR. Along with that, the CFLOG model obtained slightly increased TCR values. However, the DFA-AOKGE

TABLE 2. CO and TCR outcomes of the DFA-AOKGE system with other models under various users.

No. of Users	FAuB Model	CFLOG Model	DFA-AOKGE
Computational Overhead (KB)			
10	6.380	10.015	12.741
20	7.107	10.378	12.014
30	7.834	11.287	14.922
40	8.924	11.833	15.650
50	9.470	11.833	14.559
60	9.833	12.378	15.650
70	10.197	13.105	15.650
80	10.560	14.195	16.013
90	10.924	13.650	18.921
100	11.287	14.377	18.194
Total Change Rate (%)			
10	8.060	38.311	49.739
20	8.060	39.656	55.790
30	6.715	42.345	57.134
40	8.060	46.378	55.790
50	12.093	50.412	57.807
60	13.438	50.412	57.807
70	12.765	55.790	71.252
80	10.749	59.823	74.613
90	13.438	57.134	75.957
100	14.110	59.823	79.991

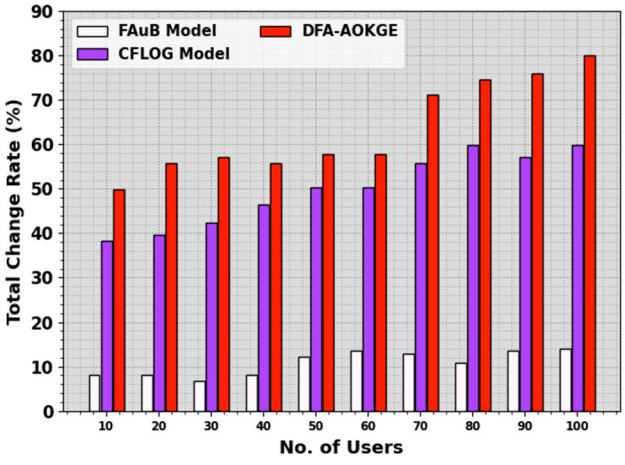


FIGURE 7. TCR analysis of the DFA-AOKGE system under various users.

system accomplishes enhanced results with increased values of TCR under all users.

In Table 3, a brief comparison analysis of the DFA-AOKGE technique with existing models is provided. Fig. 8 offers a comparative key generation time (KGT) results of the DFA-AOKGE technique with CB-EL GAMAL and Paillier models take place. The results imply that the DFA-AOKGE technique reaches reduced KGT values over all users. For instance, with 10 users, the DFA-AOKGE technique provides minimal KGT of 37.92ms while the CB-EL GAMAL and Pailler models obtain increased KGT values of 50.31ms and 537.79ms, respectively.

TABLE 3. KGT, ET, and DT outcome of DFA-AOKGE approach with other methods under various users.

No. of Users	DFA-AOKGE	CB-EL GAMAL	Paillier Model
Key Generation Time (ms)			
10	37.92	50.31	537.79
20	24.13	49.97	548.13
30	41.37	50.76	558.47
40	34.48	49.86	555.02
50	34.48	51.21	561.92
60	34.48	50.31	551.57
70	34.48	50.31	555.02
80	44.82	48.52	558.47
90	37.92	49.86	561.92
100	44.82	49.86	558.47
Encryption Time (ms)			
10	22.66	43.64	250.52
20	33.15	48.14	250.52
30	13.66	45.14	246.02
40	21.16	51.14	250.52
50	33.15	54.14	243.02
60	30.15	49.64	243.02
70	30.15	61.63	246.02
80	24.15	61.63	241.52
90	24.15	60.13	249.02
100	36.15	61.63	246.02
Decryption Time (ms)			
10	37.94	60.79	285.48
20	41.75	79.84	266.44
30	34.14	79.84	274.06
40	41.75	68.41	262.63
50	34.14	64.60	277.87
60	37.94	68.41	270.25
70	53.18	83.64	262.63
80	60.79	87.45	277.87
90	45.56	87.45	296.91
100	41.75	83.64	274.06

Fig. 9 shows a comparison of encryption time(ET) analysis of the DFA-AOKGE system with CB-EL GAMAL and Paillier techniques takes place. The attained outcomes show that the DFA-AOKGE algorithm gets decreased ET values over all users. According to 10 users, the DFA-AOKGE system gives a decreased ET of 22.66ms while the CB-EL GAMAL and Pailler models gain improved ET values of 43.64ms and 250.52ms, individually.

Fig. 10 exhibits a comparison of decryption time(DT) analysis of the DFA-AOKGE method with CB-EL GAMAL and Paillier systems. The attained outcomes pointed out that

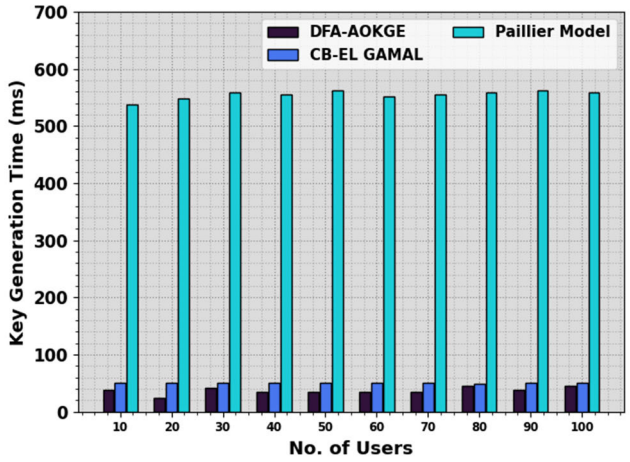


FIGURE 8. KGT analysis of the DFA-AOKGE system compared to other algorithms.

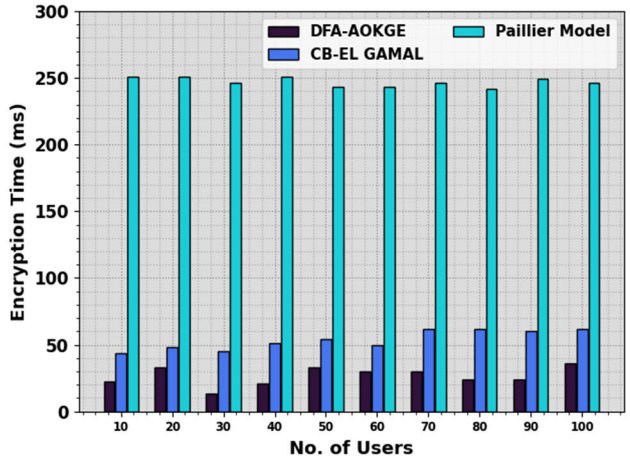


FIGURE 9. ET analysis of the DFA-AOKGE system compared to other algorithms.

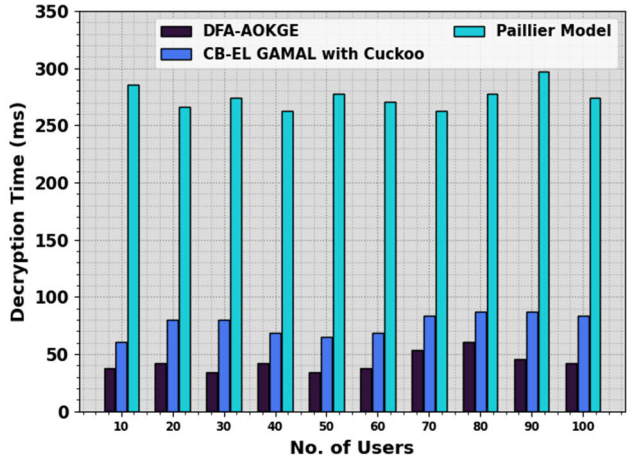


FIGURE 10. DT analysis of the DFA-AOKGE system compared to other existing models.

the DFA-AOKGE system gets minimized DT values in all users. Based on 10 users, the DFA-AOKGE algorithm gives a diminished DT of 37.94ms while the CB-EL GAMAL and Pailler models gain improved DT values of 60.79ms and 285.48ms, correspondingly. From these results, it is apparent that the DFA-AOKGE technique reaches better performance than other existing models.

V. CONCLUSION

In this article, we have developed a novel DFA-AOKGE technique to accomplish security of the digital images. The DFA-AOKGE technique makes use of a decentralized BC technology to share data among different peers for evidence collection and secure storage. By including a strong authentication device utilizing SBVM and producing optimum cryptographic keys utilizing the EEO model, this technique confirms a difficult defense besides illegal access and potential threats to image privacy. The authentication layer offers a safe gateway, permitting only official users to entree and adapt images, so justifying the danger of unofficial modifications or data breaches. The finest key generation utilizing the EEO model further supports the encryption procedure, guaranteeing that cryptographic keys are dynamic and well-produced dependent upon the single features of the images. An extensive range of experimental studies specified the supremacy of the developed model over other current techniques. The possible impact on forensic studies is important, offering enhanced data reliability, boosted privacy, and efficient access control. The model's flexibility creates it a real-world choice for boosting the safety of digital forensic data, thereby definitely influencing the efficiency of forensic investigations in real uses.

Future work must concentrate on the improvements in authentication protocols, including multi-factor authentication or biometric-based confirmation, which can additionally strengthen access control devices. Furthermore, exploring innovative encryption models and algorithms, such as homomorphic encryption or post-quantum cryptography, may donate to improving the complete flexibility of image safety. Future works must concentrate on refining authentication devices, discovering innovative encryption methods, and incorporating emerging tools to safeguard a strong, adaptive, and future-proof solution for the ever-growing loads of secure image storage and transmission.

Declarations

Ethics Approval: Not Applicable

Conflict of Interest

The author declares that they have no conflict of interest.

Data Availability Statement

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Consent to Participate

Not applicable.

REFERENCES

[1] P. M. Bachiphale and N. S. Zulpe, "Optimal multisecret image sharing using lightweight visual sign-cryptography scheme with optimal key generation for gray/color images," *Int. J. Image Graph.*, Jul. 2023, Art. no. 2550017. [Online]. Available: https://doi.org/10.1142/S0219467825500172

[2] G. Kumar, R. Saha, C. Lal, and M. Conti, "Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications," *Future Gener. Comput. Syst.*, vol. 120, pp. 13–25, Jul. 2021.

[3] L. Raji and S. T. Ramya, "Secure forensic data transmission system in cloud database using fuzzy based butterfly optimization and modified ECC," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 9, p. e4558, Sep. 2022.

[4] E. A. Abdel-Ghaffar and M. Daoudi, "Personal authentication and cryptographic key generation based on electroencephalographic signals," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 5, May 2023, Art. no. 101541.

[5] P. Velmurugadass, S. Dhanasekaran, S. S. Anand, and V. Vasudevan, "Enhancing blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm," *Mater. Today, Proc.*, vol. 37, pp. 2653–2659, 2021.

[6] V. O. Nyangaresi, M. Ahmad, A. Alkhayyat, and W. Feng, "Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things," *Expert Syst.*, vol. 39, no. 10, p. e13126, Dec. 2022.

[7] S. Nasreen and A. H. Mir, "Enhancing cloud forensic investigation system in distributed cloud computing using DK-CP-ECC algorithm and EK-ANFIS," *J. Mobile Multimedia*, vol. 19, no. 3, pp. 679–706, Feb. 2023.

[8] J. Du, S. H. Raza, M. Ahmad, I. Alam, S. H. Dar, and M. A. Habib, "Digital forensics as advanced ransomware pre-attack detection algorithm for endpoint data protection," *Secur. Commun. Netw.*, vol. 2022, pp. 1–16, Jul. 2022.

[9] A. Razaque, M. Aloqaily, M. Almiani, Y. Jararweh, and G. Srivastava, "Efficient and reliable forensics using intelligent edge computing," *Future Gener. Comput. Syst.*, vol. 118, pp. 230–239, May 2021.

[10] M. Kashif, S. Mehfuz, I. Shakeel, and S. Ahmad, "Employing an ECC-based hybrid data encryption method to improve multitenancy security in cloud computing," in *Proc. Int. Conf. Recent Adv. Electr., Electron. Digit. Healthcare Technol. (REEDCON)*, May 2023, pp. 79–83.

[11] G. Shankar, L. H. Ai-Farhani, P. A. C. Angelin, P. Singh, A. Alqahtani, A. Singh, G. Kaur, and I. A. Samori, "Improved multisignature scheme for authenticity of digital document in digital forensics using edward-curve digital signature algorithm," *Secur. Commun. Netw.*, vol. 2023, pp. 1–18, Apr. 2023.

[12] D. Unal, A. Al-Ali, F. O. Catak, and M. Hammoudeh, "A secure and efficient Internet of Things cloud encryption scheme with forensics investigation compatibility based on identity-based encryption," *Future Gener. Comput. Syst.*, vol. 125, pp. 433–445, Dec. 2021.

[13] S. Sheeja, "Towards an optimal security using multifactor scalable lightweight cryptography for IoT," in *Proc. 3rd Int. Conf. Commun., Comput. Ind. 4.0 (C2I4)*, Dec. 2022, pp. 1–6.

[14] P. S. Apirajitha and R. R. Devi, "A novel blockchain framework for digital forensics in cloud environment using multi-objective Krill Herd cuckoo search optimization algorithm," *Wireless Pers. Commun.*, vol. 132, no. 2, pp. 1083–1098, Sep. 2023.

[15] B. D. Deebak and F. AL-Turjman, "Lightweight authentication for IoT/cloud-based forensics in intelligent data computing," *Future Gener. Comput. Syst.*, vol. 116, pp. 406–425, Mar. 2021.

[16] R. Rajashree, V. Peroumal, L. Kishore, K. V. D. Reddy, S. Reddy, and M. Jagannath, "Implementation of high speed and lightweight symmetric key encryption algorithm-based authentication protocol for resource constrained devices," *Int. J. Electron. Secur. Digit. Forensics*, vol. 14, no. 3, pp. 238–263, 2022.

[17] K. M. Venkatachalam, K. Venkatachalam, P. Prabu, A. Almutairi, and M. Abouhawwash, "Secure biometric authentication with de-duplication on distributed cloud storage," *PeerJ Comput. Sci.*, vol. 7, p. e569, Jul. 2021.

[18] S. K. Henge, G. Jayaraman, M. Sreedevi, R. Rajakumar, M. Rashid, S. S. Alshamrani, M. M. Alnfiai, and A. S. AlGhamdi, "Secure keys data distribution based user-storage-transit server authentication process model using mathematical post-quantum cryptography methodology," *Netw. Heterogeneous Media*, vol. 18, no. 3, pp. 1313–1334, 2023.

[19] Z. Liu, L. Wan, J. Guo, F. Huang, X. Feng, L. Wang, and J. Ma, "PPRU: A privacy-preserving reputation updating scheme for cloud-assisted vehicular networks," *IEEE Trans. Veh. Technol.*, pp. 1–16, 2023, doi: 10.1109/TVT.2023.3340723.

[20] J. Guo, Z. Liu, S. Tian, F. Huang, J. Li, X. Li, K. K. Igorevich, and J. Ma, "TFL-DT: A trust evaluation scheme for federated learning in digital twin for mobile networks," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 11, pp. 3548–3560, Nov. 2023.

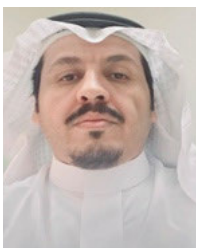
[21] Y. Miao, Y. Yang, X. Li, L. Wei, Z. Liu, and R. H. Deng, "Efficient privacy-preserving spatial data query in cloud computing," *IEEE Trans. Knowl. Data Eng.*, vol. 36, no. 1, pp. 122–136, Jan. 2024.

[22] E. H. Houssein, M. H. Hassan, M. A. Mahdy, and S. Kamel, "Development and application of equilibrium optimizer for optimal power flow calculation of power system," *Int. J. Speech Technol.*, vol. 53, no. 6, pp. 7232–7253, Mar. 2023.

[23] Y. Khan and S. Verma, "An intelligent blockchain and software-defined networking-based evidence collection architecture for cloud environment," *Sci. Program.*, vol. 2021, pp. 1–19, Sep. 2021.

[24] H. Chen, W. Dai, M. Kim, and Y. Song, "Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2019, pp. 395–412.

ABDULLAH MUJAWIB ALASHJAEE received the Ph.D. degree in computer science from the University of Idaho, USA, in 2021. He is currently an Assistant Professor with the Department of Computer Science, Northern Border University, Saudi Arabia. His research interests include mobile malware forensics, cybersecurity, digital forensics, and intrusion detection systems. Through his research, he strives to advance knowledge and understanding in these fields and contribute to the development of effective strategies and solutions. He has an exemplary track record of publications in a variety of top academic journals and conferences, demonstrating his commitment to sharing his research findings with the wider scientific community. His work has earned him recognition and respect among his peers and has contributed to advancing the field of computer science. Overall, he is a highly accomplished assistant professor known for his expertise in mobile malware forensics, cybersecurity, digital forensics, and intrusion detection systems. With a strong background in research and teaching, he strives to make a valuable contribution to these areas and inspire future generations of computer scientists.



FAHAD ALQAHTANI received the Ph.D. degree in information security from the University of Idaho, USA, in 2023. He is currently a seasoned Assistant Professor with the Department of Computer Science, Prince Sattam Bin Abdulaziz University, Saudi Arabia. He brings a wealth of knowledge and expertise to the academic realm, with a particular emphasis on cybersecurity. His research is multifaceted, delving into crucial aspects of cybersecurity, such as malware detection, digital forensics, and cloud computing. His dedication to advancing the field is evidenced by his robust academic background and a commitment to staying at the forefront of technological developments. In addition to his research contributions, he is a highly experienced educator, having successfully taught various cybersecurity courses. This pedagogical experience not only underscores his proficiency in the subject matter but also positions him as a valuable resource for providing assistance and guidance in the dynamic and critical field of cybersecurity.