Online-Journals.org

iJOE International Journal of Online and Biomedical Engineering

iJOE | eISSN: 2626-8493 | Vol. 22 No. 2 (2026) | OPEN ACCESS

https://doi.org/10.3991/ijoe.v22i02.58239

PAPER

ZTX-BAIC: A Multi-Layered Cloud Security Framework Integrating ZTA Extended with Blockchain, AI, Advanced Encryption, and CSPM

M R H Khan[1], Md Masud Rana[2] (✉), Mir Mehedi Rahman[1]

[1]Emporia State University, Emporia, KS, USA

[2]San Juan College, Farmington, NM, USA

ranam@sanjuancollege.edu

ABSTRACT

With the advancement of modern technology, enterprises are migrating to cloud computing to accelerate innovation in an increasingly competitive global landscape. Despite its benefits, cloud computing is encountering highly escalating cyber threats, such as identity theft, data breaches, cyber vandalism, and social engineering. This study proposes ZTX-BAIC, an integrated comprehensive framework for cloud security that converges the idea of zero trust architecture (ZTA), generative AI-driven threat detection, blockchain-based auditable security and smart contracts, cloud security posture management (CSPM), and advanced encryption. In the proposed framework, ZTA enforces perpetual authentication and privilege-based access control while the blockchain reinforces security systems utilizing identity management and tamper-resistant audit logging. Generative AI (GenAI) and CSPM are integrated to detect possible real-time threats with high accuracy and to generate automated compliance reports. The technology acceptance model (TAM) is utilized to validate the practical deployment of this framework. This study critically fills gaps in existing cloud security practices. The proposed design offers an adaptive, diversified, multi-layered defensive model that ensures behavioral adaptation and technical sophistication. While previous models have employed ZTA, blockchain, or generative AI in isolation or combining a couple of them, this study integrates the mentioned techniques into a cohesive and unified cloud security framework.

KEYWORDS

cloud security, zero trust architecture (ZTA), blockchain, generative AI (GenAI), cloud security posture management (CSPM), technology acceptance model (TAM)

1 INTRODUCTION

In a rapidly changing digital landscape, staying competitive drives enterprises to adopt cloud computing services. Enterprises can enhance operational efficiency,

Khan, M. R. H., Rana, M. M., Rahman, M. M. (2026). ZTX-BAIC: A Multi-Layered Cloud Security Framework Integrating ZTA Extended with Blockchain, AI, Advanced Encryption, and CSPM. *International Journal of Online and Biomedical Engineering (iJOE)*, 22(2), pp. 124–141. https://doi.org/10.3991/ijoe.v22i02.58239

Article submitted 2025-08-14. Revision uploaded 2025-11-11. Final acceptance 2025-11-12.

reduce costs, and maintain a competitive edge using cloud computing services [1]. Cloud computing is not only essential technology for Fortune 500 companies, also known as large enterprises (LEs), but also for small and medium enterprises (SMEs) as well due to its organizational agility and operational efficiency. However, the increased adoption of cloud services has introduced cybersecurity risks, including data breaches, unauthorized access, insider threats, and misconfigurations [2]. Cybersecurity has become a critical concern for both public and private sectors because of the growing frequency and severity of cybercrime in cloud environments. From LEs to SMEs, from traditional manufacturers to leading-edge tech firms, no enterprise is resistant to cyber threats. In 2024, the average cost of a data breach reached an all-time high of $4.88 million. It is estimated that cybercrime will damage over $10.5 trillion worth of enterprise assets globally, and ransomware payments will exceed $265 billion annually by 2031 [3].

The April 2025 cyberattacks on Australia's largest pension fund exposed more than 20,000 member accounts, which attempted to steal A$4.2 trillion ($2.63 trillion) in retirement savings from multiple accounts [4]. In 2024, hackers accessed cloud environments hosted on Snowflake Inc. and stole a variety of sensitive information, including over 50 billion AT&T call records and text messages [5]. The 2023 ransomware and cyberattack on Ukraine's leading telecommunications company, Kyivstar, resulted in approximately $90 million in recovery costs [6]. In 2023, MOVEit, by Progress Software Corporation, was hacked, and data was stolen by a ransomware operation called Cl0p, exposing personal data of 2,700 organizations, including education, healthcare, and finance, and approximately 93 million individuals [7].

Traditional parameter-based security architecture has proven inadequate and ineffective against sophisticated cyber threats. Consequently, enterprises seek innovative and adaptive security solutions to protect their assets from cybercriminals. Zero trust architecture (ZTA) has gained traction in recent years due to its "never trust, always verify" principle [1], [8]. ZTA challenges the conventional idea of implicit trust; rather, it has a strict policy of enforcement that no user or device is implicitly trusted, regardless of stature or location. Nevertheless, ZTA alone is inadequate to protect against emerging sophisticated cyber threats. Therefore, complementing it with other advanced security technologies becomes essential.

Blockchain technology, widely recognized for its immutability and decentralization, has recently been explored for auditable security because it ensures data integrity and tamper resistance [9]. Unlike traditional access control systems, blockchain-based auditable security ensures accountability in access control enforcement and prevents tampering to ensure all access control decisions are permanently recorded, reducing insider threats [10]. Additionally, integration of generative artificial intelligence (GenAI)-driven threat detection methods makes ZTA stronger by mitigating real-time cyber threats. This method utilizes advanced algorithms, deep learning (DL), and machine learning (ML) techniques to identify evolving attack patterns and anomalies to respond to the incident faster [11]. Even after setting up sophisticated security solutions, enterprises often encounter misconfigurations, which are one of the major causes of security vulnerabilities in cloud environments. To complement ZTA with blockchain and AI threat detection, cloud security posture management (CSPM) acts as a robust tool to monitor and automate cloud configurations to prevent security vulnerabilities caused by misconfigurations [12]. Advanced encryption plays a foundational role in this entire security framework and supports all the mentioned security tools across every security layer. It safeguards data from insider threats and unauthorized access by converting plaintext into ciphertext using cryptographic algorithms [13]. Additionally, advanced encryption secures

smart contracts on a blockchain to prevent unauthorized access and protects the training data and models that AI uses for advanced threat detection.

This study proposes an integrated cloud security framework, ZTX-BAIC (ZTA extended with blockchain, AI, and CSPM, with advanced encryption), that synergizes ZTA for zero-trust, blockchain-based audible security and smart contracts, GenAI for threat detection, CSPM to correct misconfigurations, and advanced encryption to support all security layers. The rationale for this integrated security is to leverage the strengths and provide a multi-layered defense strategy to mitigate cloud security threats and respond proactively to emerging cybersecurity challenges. The recommendations are made to protect the cloud infrastructures and support seamless operations. It is seen in the industry that the best technologies fail when users or enterprises don't see their practical value (usefulness) or find them overly complicated (ease of use). The authors integrated the technology acceptance model (TAM) [14] to evaluate the framework using a user-centric lens. TAM suggests that the proposed framework ZTX-BAIC holds strong potential for enterprise adoption.

2 LITERATURE REVIEW

2.1 ZTA, micro-segmentation, and multi-factor authentication

He et al. [1] discuss ZTA assumptions that the network is always in danger and all users, devices, network traffic, and systems need authentication before authorization. Thus, ZTA authenticates users and devices through multi-factor authentication (MFA) and access control policies. Ahmadi [15] examines ZTA and suggests the least privileged access to restrict users and devices to access only necessary resources to complete the tasks and MFA to add verification layers to reinforce identity and access management (IAM). Mali [16] illustrates that MFA mitigates identity theft and cyberattacks by requiring independent dimensions verification.

2.2 Blockchain for auditable security, identity management, and contracts

Kassen [17] explains blockchain as a set of uniquely distributed multidimensional databases that sequentially record data as blocks. Thus, blockchain-based decentralized identity management (DIM) can be used to leverage distributed ledger technology to eliminate dependence on centralized databases [18], [19]. Users can control their identities autonomously without relying on centralized authority by managing decentralized identifiers (DIDs) [20], [21]. Dunphy and Petitcolas [19] discuss that it ensures personal data is inaccessible to third parties, making it resilient to data breaches. Deshmukh et al. [22] investigate the application of smart contracts in cloud-based insurance systems and demonstrate how event-driven smart contracts automate the whole claims lifecycle from commencement to reimbursement.

2.3 Generative AI for advanced threat detection

Generative AI has been progressively integrated into cybersecurity frameworks due to its enhanced capability to detect and address complex cyber threats. Patel et al. [23] highlight GenAI's ability to identify risks with 97% accuracy, substantially surpassing the accuracy of conventional models. Its strengths include anomaly

detection, proactive threat simulation, and real-time incident response, essential for dynamic cloud environments. However, GenAI heavily depends on the quality and diversity of its training datasets, and its deployment requires significant computational resources [11].

2.4 CSPM and advanced encryption

Metibemu et al. [12] and Ofili et al. [24] discuss that CSPM provides continuous monitoring and automatic audits, ensuring cloud infrastructure complies rigorously with defined security policies. When integrated with ZTA, CSPM substantially improves compliance and mitigates risks associated with misconfigurations. Advanced encryption techniques form the backbone of safe cloud environments, providing robust protection for data at rest, in transit, and during processing. Dyavani and Thanjaivadivel [13] and Polam et al. [25] describe homomorphic encryption and quantum-resistant algorithms to ensure data security even in instances of unauthorized access.

2.5 Integration of TAM for adoption analysis

Technology acceptance model is employed to assess user acceptance and organizational adoption. Davis et al. [14] explain that TAM consists of perceived usefulness (PU) and perceived ease of use (PEOU) as critical factors influencing the adoption of technology. TAM in this study examines the behavioral aspects of framework adoption and interplay between technological and human factors [26] with the increasing scholarly focus on technology acceptability in cybersecurity implementations. ZTX-BAIC's PU is derived from its capacity to prevent data breaches, enforce least-privilege access, automate threat responses, and ensure auditability. The PEOU relates to the effortless integration of these technologies into existing infrastructures. Table 1 summarizes the literature reviewed, identifies gaps not addressed in existing studies, and highlights how this study contributes through the ZTX-BAIC framework.

Table 1. Contributions through the security framework to fill the study gap

Sl.	Author(s) and Year	Journal	Key Findings on ZTA and Cloud Security	How This Research Fills the Gap
1	He et al. (2022)	*Wireless Communications and Mobile Computing*	Defined ZTA principles; emphasized continuous verification.	Proposes an integrated ZTA framework enhanced by generative AI and blockchain for comprehensive cloud security.
2	Putz et al. (2019)	*Computers & Security*	Presented blockchain for secure event logging, auditability, and accountability.	Combines blockchain with ZTA principles and generative AI for cloud security management.
3	Akhtar et al. (2024)	*IEEE Transactions on Dependable and Secure Computing*	Proposed blockchain-based auditable access control.	Adds AI-driven threat detection capabilities into blockchain-based auditable security within ZTA.
4	Stockburger et al. (2021)	*Blockchain: Research and Applications*	Proposed decentralized blockchain identity management for security.	Integrates blockchain-based decentralized identity management with ZTA and AI-driven threat monitoring.
5	Dyavani & Thanjaivadivel (2021)	*Journal of Current Science*	Advocated advanced encryption techniques for cloud security.	Embeds advanced encryption seamlessly into ZTA and blockchain to ensure security.

(Continued)

Table 1. Contributions through the security framework to fill the study gap *(Continued)*

Sl.	Author(s) and Year	Journal	Key Findings on ZTA and Cloud Security	How This Research Fills the Gap
6	Ali et al. (2024)	*Journal of Computer Information Systems*	Reviewed ZTA, encryption, and risk assessment in cloud computing.	Presents an integrated framework combining ZTA, blockchain, AI, CSPM, and encryption.
7	Zhang et al. (2020)	*ACM Computing Surveys*	Attribute-based encryption for cloud access control.	Integrates encryption with ZTA, blockchain, and AI approaches.
8	Wang & Wang (2022)	*IEEE Transactions on Information Forensics and Security*	Explored MFA vulnerabilities in mobile devices.	Incorporates MFA security assessment with ZTA.
9	Kassen (2023)	*Policy & Internet*	Blockchain governance principles and opportunities.	Utilizes blockchain governance to enhance cloud security and integrates with ZTA.
10	Dunphy & Petitcolas (2018)	*IEEE Security & Privacy*	Blockchain-based identity management systems overview.	Connects DIM with ZTA and AI-driven security.
11	Peng et al. (2022)	*IEEE Transactions on Network Science and Engineering*	Blockchain-enabled federated learning for auditability.	Integrates blockchain auditability with AI-driven threat detection under ZTA principles.
12	Gousteris et al. (2023)	*Emerging Science Journal*	Blockchain-based secure cloud storage and data sharing.	Enhances secure cloud storage with AI-driven detection, ZTA, and blockchain auditing.
13	Saleem et al. (2023)	*Journal of Information Security and Applications*	ZTA for secure information processing.	Creates an integrated approach with ZTA.

3 METHODOLOGY

This study employs a design-science research (DSR) methodology [27] to develop and validate a theoretical cloud security framework. The DSR approach is well-suited for creating and evaluating innovative artifacts [28] (in this case, a conceptual cloud security framework) through iterative design and analysis. Following DSR principles, the research proceeded from problem identification and objective definition, through literature-driven conceptual modeling, to an expert-informed evaluation of the proposed framework. The methodology is organized into three main parts.

3.1 Research design

We established a structured approach grounded in DSR and contemporary cybersecurity modeling practices. First, we identified critical cloud security challenges that current approaches struggle to address. Second, we defined the objective: to design a holistic framework that integrates four advanced technologies with the ZTA framework: generative AI-driven threat detection, blockchain-based DIM and auditable logs, and CSPM with advanced encryption to mitigate the identified challenges. Third, the framework design drew on extensive literature synthesis: the authors reviewed research on each of the four core technologies and the ZTA framework and noted how each technology addresses specific cloud threats or limitations. Throughout the research design phase, we iteratively refine the framework concept and ensure that the resulting model is relevant to real-world problems.

3.2 Framework development process

The Framework Development Process proceeded through several iterative steps:

Problem Analysis and Requirements: We began by formalizing the cloud security problems to be addressed. This included analyzing scenarios of advanced persistent threats, insider threats, and configuration errors in cloud environments.

Literature Synthesis for Each Component: For each of the four technologies with ZTA, we conducted a focused literature review to gather design knowledge and best practices. This included studying the zero trust framework, such as the NIST ZTA guidelines [8], the latest developments in intrusion detection [29] (with an emphasis on generative AI models); advancements in blockchain for security (DID, smart contracts, and audit logs) [19]; and CSPM tools [12].

Conceptual modeling and integration: We designed the integrated framework architecture as a conceptual model. ZTA served as the structural foundation. The GenAI Threat Detection module continuously monitors network and user behavior (ingesting logs, API calls, etc.). Blockchain-based DIM authenticates ZTA subsystem. Simultaneously, a blockchain-based auditable logging system underpins the framework's accountability. The CSPM engine continuously scans the cloud environment for configuration drift or policy violations (e.g., open storage buckets). Advanced encryption in the zero trust model limits the damage.

Theoretical Refinement: We conducted a scenario analysis to verify that each identified challenge was addressed by at least one part of the framework. Thought experiments were applied for stolen credentials and cloud misconfiguration scenarios.

3.3 Theoretical evaluation

A theoretical evaluation was conducted in lieu of immediate implementation. This multi-faceted evaluation aimed to demonstrate the framework's validity, completeness, and potential effectiveness through analytical and expert-driven methods. The developed framework was presented to a panel of cybersecurity experts and researchers for qualitative feedback. Their feedback was positive, noting that the framework is comprehensive in covering major cloud threats. We performed an alignment analysis to ensure the ZTX-BAIC framework meets established security principles and addresses known threat categories. To further evaluate the framework's effectiveness, we crafted cloud attack scenarios (drawn from real case studies and threat reports) and walked through how the framework would handle each step of the attack.

Finally, we assessed improvements such as the expected reduction in dwell time (time an attacker remains undetected) due to GenAI's rapid anomaly reporting and enhanced compliance and audit readiness thanks to blockchain logs.

4 PROPOSED FRAMEWORK ZTX-BAIC

The proposed security framework, ZTX-BAIC (ZTA extended with Blockchain, AI, and CSPM, with Advanced Encryption), integrates cutting-edge technologies to address multifaceted challenges in cloud security, such as advanced cyber threats, identity verification issues, misconfigurations, and encryption weaknesses. The foundational framework is ZTA, which highlights a significant shift from conventional perimeter-based security to a "never trust, always verify" strategy. It employs micro-segmentation to isolate workloads into smaller, easier-to-manage

pieces, which restricts unauthorized lateral movement. GenAI integration into the ZTA enables the identification and response to new cyber threats before they occur. This allows for immediate response actions, for example, by starting extra security checks or isolating compromised segments to prevent more damage. The framework integrates blockchain technology to provide tamper-resistant audit logs and robust DIM. An immutable blockchain ledger keeps track of every security event, such as authentication attempts, access grants, policy modifications, and anomaly detections.

Cloud security posture management complements the framework by continuously monitoring cloud configurations and automatically detecting and fixing security misconfigurations. Integrating CSPM with ZTA ensures that all cloud resources follow the established security policies. Encryption is the most important part of the entire security system, as it protects data at all security layers. Advanced encryption techniques, such as homomorphic encryption and quantum-resistant cryptography, ensure that even if an attacker gains access through more advanced ways, the data remains unreadable without the correct cryptographic keys. Finally, TAM is incorporated into the proposed framework ZTX-BAIC to ensure practical adoption and effective implementation to provide a dynamic, multilayered security approach. Each technology addresses specific vulnerabilities and works well with the others to make cloud infrastructures more resilient.

5 FRAMEWORK OVERVIEW AND DISCUSSION

5.1 ZTA

Zero trust architecture, proposed by John Kindervag, principal analyst at Forrester in 2010, is a security model that considers all traffic or entities, whether from an internal or external network, untrusted by default and requires continuous verification to grant access [8]. It is a cybersecurity architecture that is based on zero-trust principles and adheres to the “never trust, always validate” principle [1]. It challenges traditional perimeter-based technology, which divides the network into internal and external networks where the firewall and intrusion detection system work as a barrier. Unlike conventional security models, ZTA does not view location as the prime factor of security stance. The foundation of ZTA includes access control, authentication [8], trust evaluation [1], encryption, and IAM [15]. Access control is essential to prevent unauthorized access to sensitive data and resources in the cloud [30], ensuring that users can maintain data confidentiality and integrity. In cloud computing, encryption technologies such as symmetric and public-key encryption control access to sensitive data, protecting it against unauthorized access or exposure. Efficacy mostly relies on the selected encryption methods, appropriate key management, and access control protocols [31], [32]. IAM works as an administrative framework for managing digital identities and access authorizations, ensuring that the right people have access to the right resources at the right times and with the right intentions [33]. As never trusting and consistently verifying is a vital principle in ZTA, organizations must establish adaptive security approaches that progress using real-time data.

Micro-segmentation is a core feature of ZTA [30]. Its granular approach within ZTA divides physical networks into isolated logical segments (micro-segments), often down to individual workloads or applications, resulting in fine-grained access control and implementing policies specific to each segment [31]. This method minimizes threat exposure, decreases network misconfigurations by 65% [34], and strengthens security against lateral attacks by preventing attackers from easily compromising

multiple systems. It establishes separate and highly secure zones inside a network, protecting workloads from unauthorized access. Figure 1 illustrates how ZTA, using micro-segmentation, employs software-defined networking (SDN) and reverse proxy. Regardless of the benefits, complex micro-segmentation implementation requires significant resources to integrate it seamlessly with existing security systems.

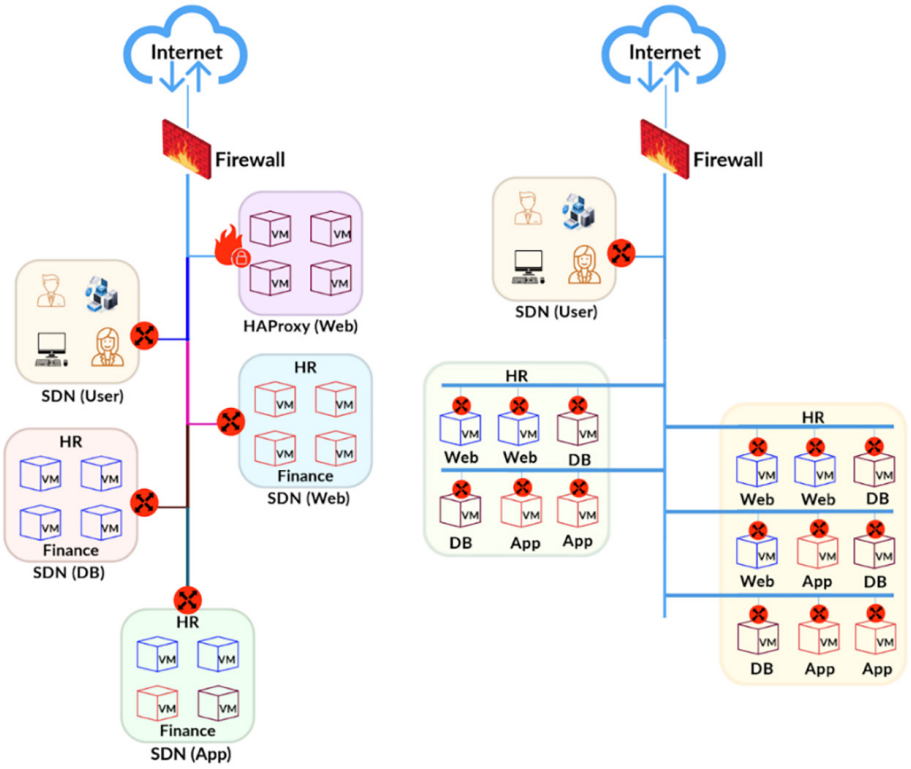

Fig. 1. Modern network security architecture integrating software-defined networking (SDN) and reverse proxy within a zero trust framework

By implementing the (i) core principles of ZTA, i.e., entity is trusted by default, (ii) micro-segmenting to divide the network into segments to restrict lateral movement, and (iii) setting a perimeter firewall at the entry point to filter traffic between the internet and internal resources, ZTA works as a robust security system.

User SDN categorizes users into isolated logical segments to enforce access controls based on roles. Database SDN (DB SDN) isolates database systems to restrict unauthorized access and safeguard sensitive data. The Application SDN (App SDN) regulates application-related traffic by isolating application resources from other components. HAProxy (Reverse Proxy) is set to replace the traditional Demilitarized Zone (DMZ). It manages web service requests, such as load balancing, SSL termination, and forwarding requests to relevant backend services. It provides an additional layer of security by masking internal server information from external users. SDN controllers dynamically enforce policies for governing communication between segments (e.g., User SDN accessing Web SDN via defined rules). Lateral movement is restricted, illustrated by a red circle and flowing arrows. If a segment (e.g., Web SDN) is breached, attackers are confined to that segment due to restricted inter-segment communication.

Each department, such as HR and Finance, is further segmented by function, with Web managing front-end services, DB dedicated to data storage and retrieval, and App overseeing backend services. This segmentation minimizes the attack surface and ensures access control at a workload level. Traffic between different functions

(e.g., HR Web to Finance DB) is rigorously regulated by policies. Unauthorized communication is blocked, illustrated by a red circle and flowing arrows. Each segment utilizes independent security measures, including authentication, encryption, and continuous monitoring. Breaches are isolated; even if one segment is compromised, others remain unaffected.

5.2 Blockchain for DIM

Blockchain-based DIM aligns with ZTA principles by enforcing strict verification mechanisms through cryptographic evidence, which significantly reduces breaches [35]. Cryptographic verification ensures that identity data remains unaltered and detectable if tampered [33]. DIM improves data protection in cloud computing by removing centralized identity repositories frequently targeted by cyberattacks [35]. Confidential information is stored off-chain, and blockchain acts as a verifier for credentials [36]. In ZTA, DIM facilitates granular access controls and adaptive authentication procedures to mitigate identity-related access control. Personal data and credentials of users are stored immutably in digital wallets. Credentials can be shared with selective service providers who verify them using blockchain without accessing the underlying data. When needed, users present cryptographic proofs to verify their identity, authenticated against blockchain records [37]. Smart contracts govern the authorization and revocation of access, assuring transparency and control [38].

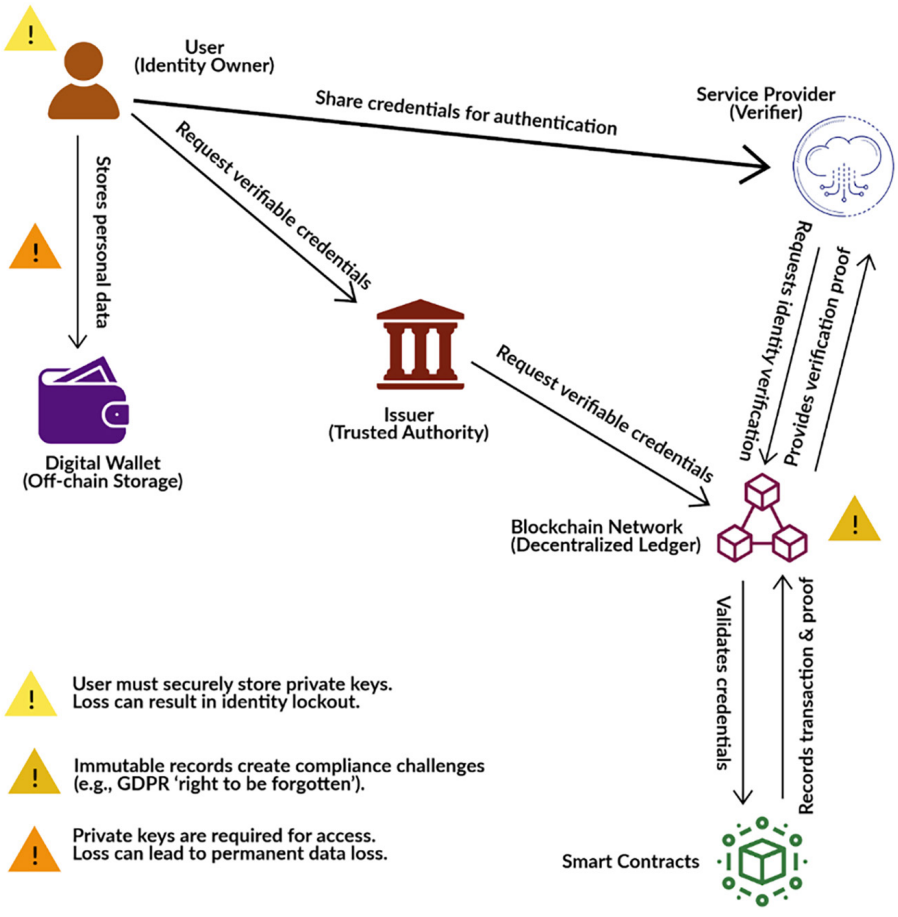

Fig. 2. Blockchain-based DIM framework with cryptographic proofs and smart contracts

Figure 2 illustrates the implementation of Blockchain-based DIM, leveraging cryptographic proofs, smart contracts, and DIDs to enhance security and reduce reliance on centralized authorities. However, users bear the responsibility of securing their private keys [39]. Scalability remains a significant barrier since public blockchains process numerous identification transactions, resulting in delays and high computational costs. SMEs find it difficult to implement DIM because it requires advanced infrastructure.

The user (identity owner) generates a decentralized identifier (DID) using a blockchain wallet and stores personal data off-chain. In Digital Wallet (off-chain storage), personal data is securely stored outside the blockchain to comply with privacy regulations, such as the GDPR. The Issuer (trusted authority) issues verifiable credentials (e.g., driver's license) linked to the DID that are cryptographically signed and stored in the user's digital wallet. Blockchain Network stores DID records and cryptographic proofs and uses smart contracts for authentication, authorization, and revocation of credentials to ensure data integrity and prevent unauthorized modifications. The Service Provider (verifier) requests identity verification from the user and verifies cryptographic proof against blockchain records without accessing personal data. It grants access based on ZTA's least privilege principles.

5.3 Blockchain for auditable security through secure event logs

Again, blockchain integration into ZTA is achieved where every participant's interaction is verified through digital signatures stored on the blockchain [39]. The zero-trust model's concept of "never trust, always verify" is strengthened by smart contracts that implement access control policies independently of centralized authority and trigger signals based on predefined security rules. The composite access control policy framework aggregates multiple access policies from different organizational domains into a single blockchain-based smart contract system. This audit access policy from multiple domains simplifies compliance with regulatory standards, as all security actions are verifiable on the blockchain, and facilitates inter-organizational collaboration [2]. Additionally, it ensures a reliable chain of custody for digital evidence, which is crucial for legal proceedings. Event logs are cryptographically authenticated by attribute managers and included in smart contracts to ensure the integrity of the logs [38]. For example, the log event and metadata are saved in a local storage cluster for efficiency and privacy. A hash of the evidence data and a timestamp are stored on the blockchain as proof of integrity. The system's private key signs and sends new log entries to the blockchain. The saved hash is compared with a new log entry hash during audits to check integrity. Matching hashes prove that the log has not changed after recording it.

Moreover, anchoring logs to a public blockchain introduces an additional layer of security, rendering it infeasible for cloud providers or attackers to alter security records undetected. Figure 3 illustrates the architecture of a blockchain-based auditable access control system. It presents two integrated layers, policy enforcement and audit verification, working in parallel. Composite policies are translated into smart contracts for immutable enforcement on the blockchain, while an audit engine and attribute manager validate and verify events to ensure integrity and compliance with zero trust principles. Blockchain's audible security is restricted by some constraints, such as that it requires significant storage capacity, and public network transactions like Bitcoin or Ethereum incur high deployment and smart contract execution costs [40].

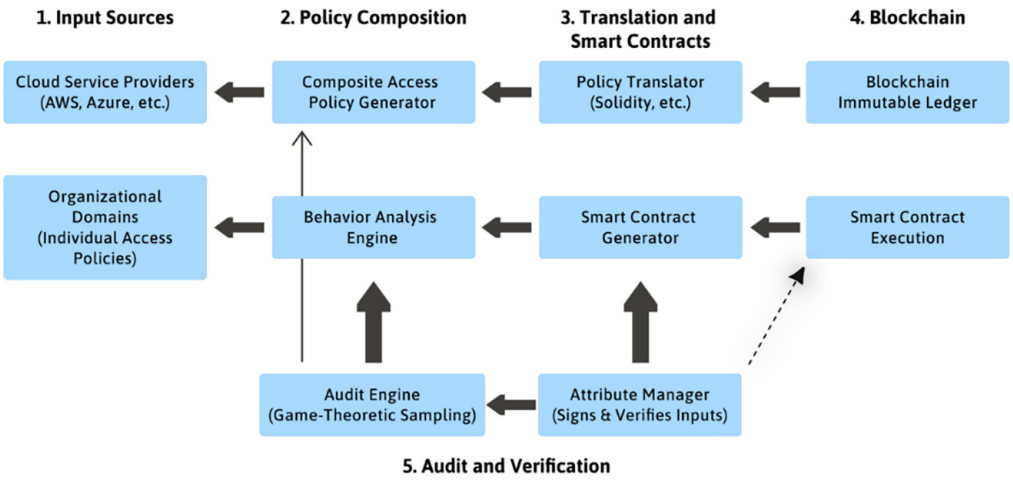

Fig. 3. Blockchain-enabled architecture for auditable and automated access control in cloud environments

A blockchain-based auditable access control in cloud environments integrates access policies from multiple organizational domains and cloud service providers into a unified policy [10]. This policy is translated into smart contracts and deployed on a blockchain to ensure tamper-resistant enforcement [37], [38]. Access events and decisions are recorded on the blockchain, supporting traceability and compliance with regulatory standards. Attribute managers verify user credentials and sign logs, which are cryptographically hashed and stored on the blockchain. The overall architecture strengthens zero-trust principles through auditable logging.

5.4 Smart contracts to automate compliance checks and incident responses

Smart contracts are executable codes deployed on a blockchain that self-execute between untrustworthy parties when predetermined conditions are met [39], [40]. These smart contracts act as decentralized programs that enforce access control, encryption, and verification mechanisms without relying on third parties. Smart contracts define and enforce service level agreements (SLAs), ensure data integrity, and manage access control to enhance security, transparency, and efficiency by reducing the manipulation risk and human error. The integration of blockchain and RSA encryption in ZTA ensures only authorized individuals can access or decode data, hence mitigating significant issues related to cloud security and privacy [25], [32].

Smart contracts effectively correspond with ZTA principles by establishing that no entity is inherently trusted [1], role-based access control maintains immutable logs [36], and that all access and operations undergo continuous verification and are executed solely according to predefined rules [34]. Users such as a hospital, insurer, patient, depositor, borrowers, or investor must authenticate using a public-private key pair [10], while smart contracts assess permissions through cryptographic credentials, and all actions are recorded on the blockchain [37]. In zero-trust environments, smart contracts function as the enforcement mechanism that verifies user credentials, validates policies, and immutably logs every interaction, thereby ensuring that no implicit trust is extended to any actor or component. The smart contract process in cloud systems has several limitations, such as RSA encryption, which exhibits relatively slow performance when applied to high-volume data operations.

5.5 GenAI for advanced threat detection

Modern cybersecurity and threat protection systems are embracing GenAI to triumph over the sophisticated, alarming cyber threats. With the significant advancement of information technology, the number of cyber threats is skyrocketing tremendously. While traditional security systems are falling short, GenAI is creating new opportunities for strengthening modern security. This emerging technology has exceptional potential to reduce security expenditure and enhance the efficiency of the overall security systems. GenAI is capable of utilizing the DL algorithm, which helps to analyze the pattern of the data, identify the anomalies, and respond to the incident faster than manual approaches [41]. GenAI consists of both ML and DL technology. The major difference between traditional AI and GenAI is that traditional AI can only predict the specific data set based on training, whereas GenAI can produce new data in various forms based on what it was trained on [42].

GenAI can have a significant impact on security threat detection through its unique features, such as synthetic data generation for simulations, anomaly reporting, incident response, and threat prediction. It is very impactful in cloud-based security systems. According to the research of Patel et al. [23], GenAI can offer 97% accuracy of threat detection, whereas the traditional model can afford only 70 to 80% accuracy. The time of threat detection and false positive rate were also very low in comparison to the conventional method [24]. There are various kinds of dynamic threats in cybersecurity, including malware attacks, ransomware, phishing, pharming, eavesdropping, advanced persistent threats, distributed denial of service (DDoS), and IoT security threats [31]. GenAI is very effective and efficient in detecting those kinds of attacks by analyzing the pattern of data and detecting anomalies and unusual activities in the systems. When trained on data from a particular organization, it can analyze patterns of regular behavior. As soon as any unusual activities are detected, it promptly responds to the incident.

5.6 CSPM and advanced encryption

Misconfigurations are one of the major causes of data breaches and security vulnerabilities in cloud environments. CSPM is an automated security solution that identifies and mitigates misconfigurations in cloud environments to prevent data breaches [12]. CSPM provides actionable insights to correct the misconfigurations and continuously monitors cloud infrastructure to ensure security compliance with regulatory standards. It scans cloud environments to detect deviations from pre-determined security policies and compliance requirements. CSPM can be integrated seamlessly with ZTA to ensure that only correctly configured and compliant resources are permitted within the network. It continuously verifies configurations and enforces least-privilege access across all cloud resources [24]. However, its effectiveness and accuracy depend on the proper rules and policy integration.

Encryption is an integral component of ZTX-BAIC that safeguards data from insider threats and unauthorized access using cryptographic algorithms that allow only authorized individuals possessing the decryption key to decipher the data [25]. Advanced encryption in ZTA ensures compliance with GDPR and PCI DSS regulatory standards through continuous validation and data protection. ZTA enhances security through identity verification and device validation [8], and continuous assessment and symmetric (AES) and asymmetric (RSA) encryption significantly reduce the risk of unauthorized access and internal threats [32], complementing

each other. Advanced encryption can be integrated seamlessly into ZTA by protecting data at rest, in transit, or in use, ensuring that even if unauthorized access occurs, the data remains secure. Together, they implement a layered defense to improve modern cloud security at multiple levels. However, limitations include performance overhead from encryption processes, particularly when handling large datasets or computationally intensive processes, which affect transaction speed and system efficiency.

5.7 Reflective integration of TAM

The TAM indicates that the proposed framework, ZTX-BAIC, offers significant PU, such as enhanced threat detection, decentralized trust management, and compliance automation. However, PEOU may vary depending on organizational readiness and behavioral intention [43]. Through TAM, the authors recognized potential barriers to integrating blockchain and advanced encryption. For example, blockchain components may be viewed as technically challenging for SMEs, but GenAI and CSPM technologies may be integrated more seamlessly with current IT infrastructures, creating PU. The improvements in threat accuracy and automated compliance could enhance PU of the framework. Organizations could initially implement CSPM with ZTA to immediately boost the framework's overall PEOU and encourage broader adoption. Thus, TAM ensures the proposed framework is technically strong and practically viable for organizations.

6 SCENARIO-BASED VALIDATION

To strengthen the practical contribution of the proposed cloud security framework, we conducted a scenario-based simulation. Three representative cloud security scenarios were modeled to illustrate how the ZTX-BAIC framework responds under realistic operational conditions. This approach aligns with established validation methods in DSR [44].

Scenario 1: Credential Compromise and Lateral Movement. An attacker acquires valid user credentials and attempts to move laterally across multiple cloud workloads. The ZTA layer enforces micro-segmentation and continuous authentication, effectively isolating each workload segment [15]. GenAI engine identifies abnormal access behaviors, such as time anomalies or unusual device profiles, and triggers policy enforcement. Meanwhile, blockchain-based secure event logs record each access attempt immutably, enhancing forensic traceability [10]. Academic evidence and industry reports document that AI-led systems achieve a 97% threat detection rate with a reduction in response latency (over 50%), reducing detection and isolation time under ZTA [23], [45], [46].

Scenario 2: Cloud Misconfiguration and Data Exposure. Cloud misconfigurations remain a leading cause of breaches [12]. In this simulated case, CSPM continuously scans configurations and detects a publicly exposed cloud storage bucket. Automated alerts are triggered, blockchain smart contracts lock access to the affected resource [40], and the GenAI engine classifies the issue as high severity, recommending immediate remediation [41]. This workflow demonstrates how automation and immutable logging prevent data exposure and improve visibility into compliance [47].

Scenario 3: Insider Threat and Unauthorized Data Access. An internal user with legitimate credentials attempts to exfiltrate sensitive data. ZTA enforces least-privilege access controls, and AI-driven anomaly detection identifies unusual data transfer behavior. Encryption ensures data confidentiality even if exfiltration occurs, while blockchain-based logs permanently record denied access attempts. Consistent with recent studies reporting up to a 70% reduction in incident response time when AI-driven detection and automated response are deployed and reducing mean time to respond (MTTR) to seconds [48], [49], the modelled scenario indicates a substantial decrease in insider-threat detection and containment time. Thus, integrating GenAI, automation, and ZTA minimizes potential damage and improves accountability by enabling faster detection and shorter response times, sometimes down to seconds in best-case deployments.

These simulation results demonstrate the operational feasibility and adaptive strength of the proposed ZTX-BAIC framework. By combining multiple technologies under a unified zero trust model, the architecture enhances detection speed, auditability, and compliance.

7 CONCLUSION

This study proposes ZTX-BAIC, a cloud security framework that integrates ZTA, GenAI-driven threat detection, blockchain-based auditable security and smart contracts, CSPM, and advanced encryption to address increasing cyber threats. The findings underscore the effectiveness of ZTA with other security technologies that complement ZTA in strengthening against cyber threats, particularly in cloud environments. The research fills the gaps in identifying robust security technologies and integrates them into a cohesive and practical cloud security framework. The comprehensive and multi-layered framework proactively addresses a wide range of security threats, including unauthorized access, insider threats, and misconfigurations.

Zero trust architecture ensures continuous verification, while GenAI proactively identifies and rapidly responds to previously unknown threats and handles incidents with accuracy. Blockchain technology with DIM and immutable audit logging improves accountability. CSPM ensures continuous configuration monitoring and rapid vulnerability repair. Throughout operations, homomorphic encryption and quantum-resistant cryptography protect sensitive data. Further, TAM adds organizational adoption potential with PU and PEOU to influence acceptance. The framework is technically robust and practically implementable in diverse organizational contexts, such as healthcare, finance, insurance, and government defense. Future research could focus on testing and empirical validation of ZTX-BAIC through organizational implementation.

8 REFERENCES

[1] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," *Wirel. Commun. Mob. Comput.*, vol. 2022, no. 1, p. 6476274, 2022. https://doi.org/10.1155/2022/6476274

[2] Z. Peng *et al.*, "VFChain: Enabling verifiable and auditable federated learning via blockchain systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 173–186, 2022. https://doi.org/10.1109/TNSE.2021.3050781

[3] P. Gratton, "10 ways cybercrime impacts business," *Investopedia*, 2025. [Online]. Available: https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx

[4] C. Chen, "Hackers strike Australia's largest pension funds in coordinated attacks," *Reuters*, 2025. [Online]. Available: https://www.reuters.com/technology/cybersecurity/multiple-australian-pension-funds-hit-by-coordinated-hacking-media-reports-say-2025-04-04/

[5] M. Egan and S. Lyngaas, "Nearly all AT&T cell customers' call and text records exposed in a massive breach," *CNN*, 2024. [Online]. Available: https://edition.cnn.com/2024/07/12/business/att-customers-massive-breach

[6] Reuters, "Ukraine's Kyivstar allocated $90 million to deal with cyberattack aftermath," *Reuters*, 2024. [Online]. Available: https://www.reuters.com/technology/cybersecurity/ukraines-kyivstar-allocated-90-million-deal-with-cyberattack-aftermath-2024-05-20/

[7] Z. Simas, "Unpacking the MOVEit breach: Statistics and analysis," *Emsisoft*, 2023. [Online]. Available: https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/

[8] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," National Institute of Standards and Technology, 2020. https://doi.org/10.6028/NIST.SP.800-207

[9] B. Putz, F. Menges, and G. Pernul, "A secure and auditable logging infrastructure based on a permissioned blockchain," *Comput. Secur.*, vol. 87, p. 101602, 2019. https://doi.org/10.1016/j.cose.2019.101602

[10] A. Akhtar *et al.*, "Blockchain based auditable access control for business processes with event driven policies," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 5, pp. 4699–4716, 2024. https://doi.org/10.1109/TDSC.2024.3356811

[11] V. R. Saddi, S. K. Gopal, A. S. Mohammed, S. Dhanasekaran, and M. S. Naruka, "Examine the role of generative AI in enhancing threat intelligence and cyber security measures," in *2024 2nd International Conference on Disruptive Technologies (ICDT)*, Greater Noida, India: IEEE, 2024, pp. 537–542. https://doi.org/10.1109/ICDT61202.2024.10489766

[12] O. C. Metibemu, T. O. Adesokan-Imran, A. J. Ajayi, O. J. Tiwo, A. T. Olutimehin, and O. O. Olaniyi, "Developing proactive threat mitigation strategies for cloud misconfiguration risks in financial SaaS applications," *J. Eng. Res. Rep.*, vol. 27, no. 3, pp. 393–413, 2025. https://doi.org/10.9734/jerr/2025/v27i31442

[13] N. R. Dyavani and M. Thanjaivadivel, "Advanced security strategies for cloud-based e-commerce: Integrating encryption, biometrics, blockchain, and zero trust for transaction protection," *J. Curr. Sci.*, vol. 9, no. 3, 2021.

[14] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User acceptance of computer technology: A comparison of two theoretical models," *Manag. Sci.*, vol. 35, no. 8, pp. 982–1003, 1989. https://doi.org/10.1287/mnsc.35.8.982

[15] S. Ahmadi, "Zero trust architecture in cloud networks: Application, challenges and future opportunities," *J. Eng. Res. Rep.*, vol. 26, no. 2, pp. 215–228, 2024. https://doi.org/10.9734/jerr/2024/v26i21083

[16] S. Mali, "Assessing the effectiveness of multi-factor authentication in cloud-based big data environments," *Internet Things Cloud Comput.*, vol. 12, no. 2, pp. 17–27, 2024. https://doi.org/10.11648/j.iotcc.20241202.11

[17] M. Kassen, "Prospects of blockchain governance: Understanding key public values, principles, challenges, and opportunities," *Policy Internet*, vol. 16, no. 1, pp. 33–64, 2024. https://doi.org/10.1002/poi3.365

[18] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala, and M. Avital, "Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation," *Blockchain Res. Appl.*, vol. 2, no. 2, p. 100014, 2021. https://doi.org/10.1016/j.bcra.2021.100014

[19] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Secur. Priv.*, vol. 16, no. 4, pp. 20–29, 2018. https://doi.org/10.1109/MSP.2018.3111247

[20] A. Satybaldy, A. Hasselgren, and M. Nowostawski, "Decentralized identity management for e-health applications: State-of-the-art and guidance for future work," *Blockchain Healthc. Today*, 2022. https://doi.org/10.30953/bhty.v5.195

[21] R. Xiong, W. Ren, X. Hao, J. He, and K.-K. R. Choo, "BDIM: A blockchain-based decentralized identity management scheme for large scale internet of things," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 22581–22590, 2023. https://doi.org/10.1109/JIOT.2023.3303922

[22] A. A. Deshmukh *et al.*, "Event-based smart contracts for automated claims processing and payouts in smart insurance," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 4, 2024. https://doi.org/10.14569/IJACSA.2024.0150486

[23] A. Patel, R. C. Sachan, H. Ragothaman, A. Sheth, P. Pandey, and S. K. Udayakumar, "Leveraging generative AI for proactive cybersecurity threat detection in cloud environments," in *2025 8th International Conference on Information and Computer Technologies (ICICT)*, Hawaii-Hilo, HI, USA: IEEE, 2025, pp. 80–85. https://doi.org/10.1109/ICICT64582.2025.00019

[24] B. T. Ofili, E. O. Erhabor, and O. T. Obasuyi, "Enhancing federal cloud security with AI: Zero trust, threat intelligence and CISA Compliance," *World J. Adv. Res. Rev.*, vol. 25, no. 2, pp. 2377–2400, 2025. https://doi.org/10.30574/wjarr.2025.25.2.0620

[25] R. M. Polam, B. Kamarthapu, A. B. Kakani, S. K. K. Nandiraju, S. K. Chundru, and S. R. Vangala, "Data security in cloud computing: encryption, zero trust, and homomorphic encryption," *Int. J. Emerg. Trends Comput. Sci. Inf. Technol.*, vol. 2, no. 1, pp. 70–80, 2021. https://doi.org/10.63282/3050-9246.IJETCSIT-V2I3P108

[26] P. Legris, J. Ingham, and P. Collerette, "Why do people use information technology? A critical review of the technology acceptance model," *Inf. Manage.*, vol. 40, no. 3, pp. 191–204, 2003. https://doi.org/10.1016/S0378-7206(01)00143-4

[27] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Q.*, vol. 28, no. 1, pp. 75–106, 2004. https://doi.org/10.2307/25148625

[28] R. Jeya, H. A. Karim, and S. B. Mansor, "Artificial intelligence and mobile apps support intelligent healthcare systems for mental health services," *Int. J. Interact. Mob. Technol. (IJIM)*, vol. 18, no. 20, pp. 157–168, 2024. https://doi.org/10.3991/ijim.v18i20.50743

[29] K. M. A. Alheeti, A. A. A. Lateef, A. Alzahrani, A. Imran, and D. Al_Dosary, "Cloud intrusion detection system based on SVM," *Int. J. Interact. Mob. Technol. (IJIM)*, vol. 17, no. 11, pp. 101–114, 2023. https://doi.org/10.3991/ijim.v17i11.39063

[30] H. A. Al-Ofeishat and R. Alshorman, "Build a secure network using segmentation and micro-segmentation techniques," *Int. J. Comput. Digit. Syst.*, vol. 16, no. 1, pp. 1499–1508, 2024. https://doi.org/10.12785/ijcds/1601111

[31] T. Ali, M. Al-Khalidi, and R. Al-Zaidi, "Information security risk assessment methods in cloud computing: Comprehensive review," *J. Comput. Inf. Syst.*, pp. 1–28, 2024. https://doi.org/10.1080/08874417.2024.2329985

[32] Y. Zhang, R. H. Deng, S. Xu, J. Sun, Q. Li, and D. Zheng, "Attribute-based encryption for cloud computing access control: A survey," *ACM Comput. Surv.*, vol. 53, no. 4, pp. 1–41, 2021. https://doi.org/10.1145/3398036

[33] J.-P. Aumasson, *Serious Cryptography: A Practical Introduction to Modern Encryption*. San Francisco, CA: No Starch Press, 2017.

[34] N. Basta, M. Ikram, M. A. Kaafar, and A. Walker, "Towards a zero-trust micro-segmentation network security strategy: An evaluation framework," in *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, Budapest, Hungary: IEEE, 2022, pp. 1–7. https://doi.org/10.1109/NOMS54207.2022.9789888

[35] S. Y. Lim *et al.*, "Blockchain technology the identity management and authentication service disruptor: A survey," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 4-2, pp. 1735–1745, 2018. https://doi.org/10.18517/ijaseit.8.4-2.6838

[36] A. Akhtar, B. Shafiq, J. Vaidya, A. Afzal, S. Shamail, and O. Rana, "Blockchain based auditable access control for distributed business processes," in *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, Singapore, Singapore: IEEE, 2020, pp. 12–22. https://doi.org/10.1109/ICDCS47774.2020.00015

[37] K. Peng, M. Li, H. Huang, C. Wang, S. Wan, and K.-K. R. Choo, "Security challenges and opportunities for smart contracts in internet of things: A survey," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 12004–12020, 2021. https://doi.org/10.1109/JIOT.2021.3074544

[38] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2901–2925, 2021. https://doi.org/10.1007/s12083-021-01127-0

[39] S. Gousteris, Y. C. Stamatiou, C. Halkiopoulos, H. Antonopoulou, and N. Kostopoulos, "Secure distributed cloud storage based on the blockchain technology and smart contracts," *Emerg. Sci. J.*, vol. 7, no. 2, pp. 469–479, 2023. https://doi.org/10.28991/ESJ-2023-07-02-012

[40] X. Ye, N. Zeng, X. Tao, D. Han, and M. König, "Smart contract generation and visualization for construction business process collaboration and automation: Upgraded workflow engine," *J. Comput. Civ. Eng.*, vol. 38, no. 6, p. 04024030, 2024. https://doi.org/10.1061/JCCEE5.CPENG-5938

[41] H. S. Mavikumbure, V. Cobilean, C. S. Wickramasinghe, D. Drake, and M. Manic, "Generative AI in cyber security of cyber physical systems: Benefits and threats," in *2024 16th International Conference on Human System Interaction (HSI)*, Paris, France: IEEE, 2024, pp. 1–8. https://doi.org/10.1109/HSI61632.2024.10613562

[42] N. Vemuri, N. Thaneeru, and V. M. Tatikonda, "Adaptive generative AI for dynamic cybersecurity threat detection in enterprises," *Int. J. Sci. Res. Arch.*, vol. 11, no. 1, pp. 2259–2265, 2024. https://doi.org/10.30574/ijsra.2024.11.1.0313

[43] R. A. Alsharida, M. M. Hammood, and M. Al-Emran, "Mobile learning adoption: A systematic review of the technology acceptance model from 2017 to 2020," *Int. J. Emerg. Technol. Learn. (IJET)*, vol. 16, no. 5, pp. 147–162, 2021. https://doi.org/10.3991/ijet.v16i05.18093

[44] T. Hoang and Y. Qu, "Creating a security baseline and cybersecurity framework for the internet of things via security controls," *Eur. J. Electr. Eng. Comput. Sci.*, vol. 8, no. 2, pp. 9–16, 2024. https://doi.org/10.24018/ejece.2024.8.2.609

[45] IBM Security, "IBM Security X-Force Threat Intelligence Index 2023," 2023. [Online]. Available: https://secure-iss.com/wp-content/uploads/2023/02/IBM-Security-X-Force-Threat-Intelligence-Index-2023.pdf

[46] Securonix, "NEC Asia Pacific transforms security operations with securonix unified platform," *Securonix*, 2025. [Online]. Available: https://www.securonix.com/wp-content/uploads/2025/07/NEC-Asia-Pacific-Transforms-Security-Operations-with-Securonix-Unified-Platform-case-study-070725_B-1.pdf

[47] S. Sharma, "Understanding the role of misconfigurations in data breaches in cloud environments," *Fidelis Cybersecurity*, 2025. [Online]. Available: https://fidelissecurity.com/threatgeek/threat-detection-response/cloud-misconfigurations-causing-data-breaches/

[48] Syracuse University School of Information Studies, "AI in cybersecurity: How AI is changing threat defense," Syracuse University School of Information Studies, 2025. [Online]. Available: https://ischool.syracuse.edu/ai-in-cybersecurity/

[49] P. Mishra, "Automated threat detection and response," *Seceon Security for Eons*, 2025. [Online]. Available: https://seceon.com/automated-threat-detection-and-response/

9 AUTHORS

M R H Khan is with the School of Business & Technology, Emporia State University, Emporia, Kansas, United States of America.

Md Masud Rana is with the School of Business, Information Technology and Social Sciences, San Juan College, Farmington, New Mexico, United States of America (E-mail: ranam@sanjuancollege.edu).

Mir Mehedi Rahman is with the School of Business & Technology, Emporia State University, Emporia, Kansas, United States of America.