Volume 12, No.9, September 2025

Journal of Global Research in Mathematical Archives

ISSN 2320 – 5822

UGC Approved Journal

RESEARCH PAPER

Available online at http://www.jgrma.info

CRYPTOGRAPHIC FOUNDATIONS OF CLOUD SECURITY: A SURVEY ON TRUST MODELS AND ZERO-KNOWLEDGE PROOF-BASED AUTHENTICATION

Neha Upadhyay[1]

[1] Assistant Professor, Department of Computer Applications, IIS University, Bhopal (M.P.)
neha.upadhyay887@gmail.com

Abstract: Cloud data storage helps people keep huge amounts of data on demand and for a low price. However, ensuring users can access the data safely and privately remains a significant challenge. Existing solutions to the problem of data privacy using cryptographic role-based access control (RBAC) systems often suffer from issues such significant computational overhead, reliance on trust, and inability to guarantee fair authorization and safe data retrieval. This study introduces a paradigm for trust-enhanced access control that integrates blockchain with searchable attributes-based encryption. It offers decentralized, transparent, and tamper-resistant access management, which is a solution to these problems. Furthermore, to improve decision-making in real-time, offer a data-oriented risk-based access control model that integrates dynamic risk assessment across subject, resource, and environmental factors. investigate new cryptographic trust models (such as blockchain, web-of-trust, and Zero-Knowledge Proofs, or ZKPs) and other emerging technologies to see whether they can provide safe authentication without revealing secret credentials. Cloud access gateways are proposed to localize trust and reduce reliance on vulnerable centralized architectures. Also, examine the limitations of current Access Control as a Service (ACaaS) and PKI-based authentication solutions. Finally, present a blockchain-based framework that combines smart contracts, distributed ledgers, and cryptographic protocols to ensure decentralized access control, privacy preservation, and auditability. It clouds service providers to deploy scalable, secure, and privacy-respecting systems, fostering broader adoption in sensitive application domains.

Keywords: Cloud computing, Access Control as a Service (ACaaS), Cryptographic Trust Models, Role-Based Access Control (RBAC), Public Key Infrastructure (PKI), Blockchain.

1 INTRODUCTION

Cloud computing has quickly become a game-changing technology. It allows customers all over the world to access scalable and affordable computational resources and data storage through third-party providers called Cloud Service Providers (CSPs) [1]. Through the use of only an internet-connected terminal, powerful infrastructure, platforms and applications are made available to the users and the administration of the underlying hardware is not provided [2]. Nonetheless, cloud computing presents massive security and privacy concerns [3] despite the cost advantages and operational efficiency. When data leaves the user's physical possession and ends up on a third party's infrastructure, it becomes susceptible to security breaches, insider threats, and unauthorized access. Information in the cloud can be subjected to a few threats such as malicious actions of CSP, business spying, or hidden information loss, which poses a threat to data precedence and trust.

Cryptography plays a crucial role in protecting information. Founded on archaic customs of communicating in mysterious codes (as Greek roots suggest, secret writing), contemporary cryptography provides us with a guarantee that confidential information not passed on to unauthorized individuals [4]. It supports safe communications and authorizations, as well as data integrity within cloud settings [5]. Yet cryptographic systems may also be weak and susceptible to their slight implementation errors. The Zero-Knowledge Proof is one of the more complex cryptographic techniques that have recently emerged for use in cloud security. The prover can use ZKPs to persuade the verifier that he is knowledgeable about something without really disclosing the information that is kept [6]. Under this approach, privacy and trust are substantially served since sensitive details are not revealed in the verification process. ZKPs have the potential to provide an effective method for secure authentication and access control in cloud testing systems, as information confidentiality is a major threat factor in such systems.

ACaaS is also a complementary concept which simplifies things in terms of authentication and authorization in the cloud [7]. Access control logic of ACaaS is done outside, and controlled by third party thus centralized policy to be implemented, less complexity of application development and support of single sign-on [8]. It operates at the application layer, delivering authentication tokens that contain authorization claims and ensure secure, unrestricted access to various cloud services.

Nevertheless, there is cloud computing reluctance on the part of enterprises. Most organisations worry about loss of control of their information especially the unlikelihood of applying their security policies after transfer of their assets to other administrations through outsourcing to third party entities [9]. Such issues support the necessity to have a strong cryptographic model of trust and sophisticated validation mechanism like ZKPs, that can bring in trust and enhance security of a cloud platform.

This review summarizes the cryptographic trust models and ZKPs that can increase the use of secure access control in the cloud. Although cloud computing is flexible and cost-effective, data privacy issues and data governance have also been raised whereby there is the threat that data on cloud lost or they compromised. This is necessary to develop trust and to securely adopt the idea of integrating cloud services.

1.1 Organization of the paper

The paper organization is the following: Section 2 is a review of the basics of cloud security fundamentals; section 3 is entitled Secure the cloud utilizing cryptographic trust models; section 4 is an outline of how to incorporate the use of ZKPs in Cloud Access Control and Authentication; section 5 is the literature review, and Section 6 is the paper conclusion with conclusion findings and directions.

2 CLOUD SECURITY

Cloud security is the process of securing information, programs and infrastructure in the cloud-based systems using safety policies, encryption, access control and surveillance. It provides confidentiality, integrity, and availability of resources regardless of whether there is a public, a given company, or a hybrid cloud. Security roles are distributed between cloud providers and users, and such measures as authentication, firewalls, and compliance standards serve to prevent the occurrence of data break, unauthorized access. The components of a cloud computing architecture include user interfaces, backend systems, service types (IaaS, PaaS, SaaS), and deployment models (public, private, hybrid, community). It facilitates on-demand, elastic availability of shared computing resources over the internet, along with introducing complicated security concerns owing to its characteristic distributed, multi-tenant nature.

2.1 Role of Cryptography in Cloud Security

Cryptography is essential in cloud security as it encrypts information, thereby protecting it from unauthorized access, and enables the decryption of scrambled data for authorized persons. In the cloud, its two fundamental goals are confidentiality, integrity and availability. Confidentiality protects sensitive information and system components, including the virtual machine images and even the managers and runs the information against unauthorized people who may tamper with information [10]. In ensuring data integrity, data is not modified, altered or corrupted in its lifetime and it is thus untamperable and trusted, hence protecting it through mechanisms such as hashing or backups. The availability provides timely data and services access without downtime, which may give large losses; it can be maintained by Service Level Agreements (SLAs), redundancy and fault-tolerant systems [11]. Symmetric and asymmetric cryptographic algorithms make secure communication, authentication and data protection possible, thus providing a basis of confidence among the cloud providers and users.

2.2 Key applications

The subsections below outline important application domains that ZKPs are central in enhancing authentication, access control, and data privacy:

2.2.1 Cloud Identity and Access Management (IAM)

Zero-Knowledge Proofs (ZKP) are a security measure that may be used to strengthen Identity and Access Management (IAM). ZKP enables users to authenticate without divulging any sensitive information, which helps to prevent phishing and data breaches [12]. Privacy-preserving role and attribute-based access controls can be used with ZKP-based IAM systems [13]. The standard IAM system consists of three entities namely data, functionalities and policies. Centralized IAM helps prevent over-privileged access and enforce security policies in distributed cloud environments.

2.2.2 Secure Federated Identity Systems

Systems for federated identities. By utilising federated identity systems, users are able to access many services with a single identity while yet maintaining control over their data. In such schemes as Project Liberty, identity providers in a circle of trust, ensure that identities established in one service are safely associated with identities in another service. Client-Side Federation improves privacy by making identity mappings be known only to the client so that exposure would not be possible even when identity and service providers collude. These systems strike a compromise between security, convenience and privacy in the cloud world.

2.2.3 Confidential Blockchain Smart Contracts

Confidential blockchain smart contracts refer to self-governing programs that automate a set of agreement terms as per the preset conditions by following an if-then logic [14]. Not legal documents but instead, coded protocols, they guarantee verifiability, timestamped and tamper-proof execution on the blockchain. Secure and automated see-saw transactions between parties are made possible by these contracts through the use of privacy-preserving mechanisms like zero-knowledge proofs [15].

2.2.4 Healthcare, Finance, and Government Cloud Services:

ZKPs facilitate compliance-oriented industries, such as healthcare, finance, and government by providing access to sensitive information without revealing the content of their records to the outside world. As another example, insurance eligibility and age of the patient could be proven without relying on revealing the complete medical history, and creditworthiness of a financial customer could be checked without having to release intimate details of income or identity. ZKPs can enable such industries to achieve high regulatory compliance, including GDPR and HIPAA.

2.3 Key Challenges for Secure Cloud Computing

The following are among the prominent risks that are depicted by cloud computing some of which cause the delays of services and some of which provided the chances to be settled with due attention and concern:

- **Security and Privacy:** One of the most urgent issues is to provide data security and user privacy. Another one would be to keep the center of sensitive data in the organization but the use of cloud services to process or access [16]. A hybrid cloud model is commonly embraced to facilitate this trade-off between scale and control.
- **Lack of Standardization:** The problem is the fact that whereas cloud platforms offer documented interfaces, they do not share common and universally applicable standards, implying that cloud providers enjoy limited interoperability. Groups such as the open grid forum and the open cloud consortium are busy implementing open standards and best practices.
- **Evolving User and System Requirements:** The key challenge faced by cloud environments and particularly by a public cloud is the ability to keep up with ever-altering user demands and a modification of technology in the spheres of networking, storage, and the interface design [17]. This continuous change has presented a problem in stability of performance, security, and compatibility.
- **Compliance and Regulatory:** The need to store a specific sort of data in the infrastructure of an organization often comes as a necessity to meet the compliance requirements established by the industry. This has led to the rise in adoption of hybrid cloud deployments, which can be both regulatory compliant, as well as having access to scalable cloud services.

3 SECURING THE CLOUD WITH CRYPTOGRAPHIC TRUST MODELS

The English word "cryptography" comes from the Greek words "kryptos" (meaning "hidden writing") and "graphein" (meaning "writing"). For a long time, cryptography has been used to describe secure communication technologies that make private information unreadable to unauthorised parties. Its roots trace back to early human civilizations, where tribes and communities relied on primitive methods of secret communication to safeguard their strategies and maintain power [18]. In modern computing, cryptography has evolved into a foundational component of secure communication, particularly in cloud environments [19]. One prominent example is the Public Key Infrastructure (PKI)-based trust model, which relies on digital certificates such as X.509 certificates to authenticate users and services [20]. These certificates facilitate secure data exchange and user verification in cloud systems. However, PKI-based trust models require complete cryptographic information to compute trust metrics, which may not always align with the dynamic and subjective trust requirements of cloud users. While effective in ensuring authentication and integrity, these models can lack flexibility in representing contextual or behavioural trust aspects in cloud security scenarios.

3.1 Definition and Principles of Trust Models

Trust models outline the mechanisms through which trust is established, assessed, and upheld between entities in digital systems particularly within public key infrastructures (PKIs). These models function by distributing and validating public keys, associating them with specific identities through the use of asymmetric cryptography. This process ensures that a given public key genuinely belongs to the claimed entity, thereby enabling secure and authenticated communication [21]. Notable examples include the "web of trust" approach used in Pretty Good Privacy (PGP), and the hierarchical PKI model, which relies on a central root Certificate Authority (CA) to authenticate and verify identities (illustrated in Figure 1).

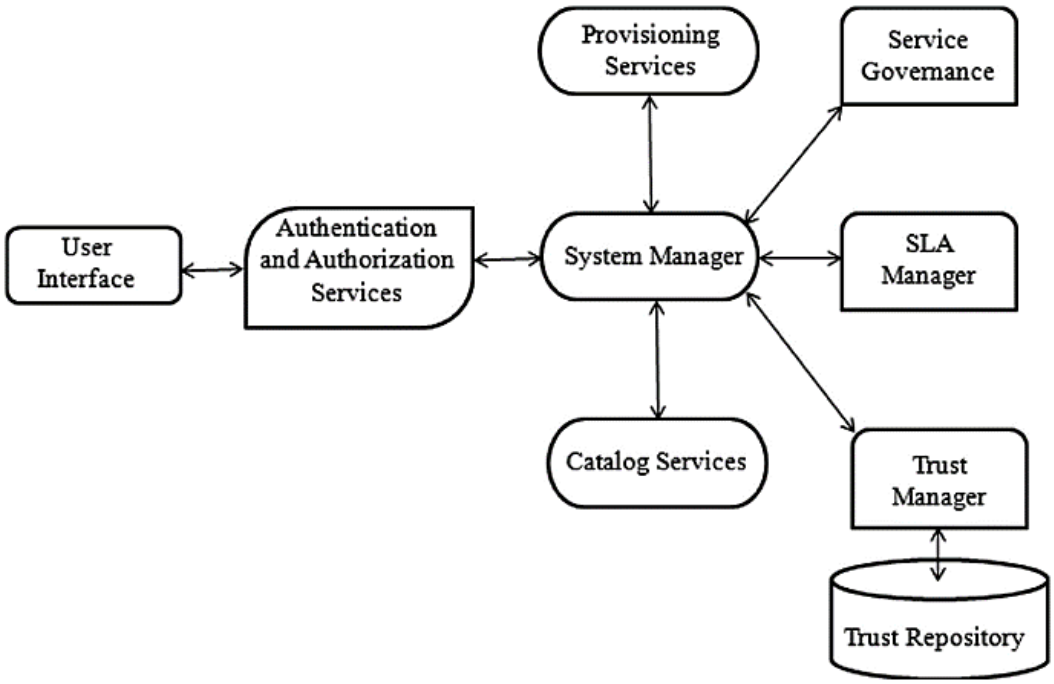

Figure 1: Trust models in cloud computing.

The Following principles/importance aspects of trust models in cryptography for cloud security are:

- **Establishing Trust Between Cloud Users and Providers:** Trust models define the security expectations and relationships between cloud service providers (CSPs) and users. As users entrust their data to third-party infrastructures, cryptographic trust models ensure data confidentiality and reliability, even when full control over the infrastructure is lacking.
- **Ensuring Data Confidentiality and Integrity:** Trust models rely on encryption, digital signatures, and cryptographic hashing to help prevent accessing (and malicious modification) of data. An example of this would be Public Key Infrastructure (PKI) which authenticates entities and keeps sensitive information accessible only to the authorized users to modify them.
- **ZKPs for Privacy-Preserving Authentication:** By using ZKPs, users are able to authenticate or prove access rights without exposing credentials. This greatly minimizes the data exposure or theft of credentials in the cloud setups.
- **PKI-Based Authentication for Secure Access:** Digital certificates are utilized to verify users and machines in PKI trust models in order to create secure connections. This method prevents threats like phishing and man-in-the-levelling attacks which tightens access security over cloud-based applications.

3.2 Centralized vs. Decentralized Trust Models

Centralized cloud computing relies entirely on data processing and storage in a single central data center, facilitated by a single cloud service provider (CSP). This architecture, makes it easy to supervise and implement policies as well as facilitates the combination of different security components as anonymization of data, steganographic and also public key encryption. The single point of failure is an inherent risk of centralisation that threatens the availability, confidentiality, and integrity of the system in the event that it fails. The data leak, or unlawful access, is another issue that is of concern in multi-tenant environments, even with the logical isolation employed.

Conversely, decentralized models of trust spread computing resources to several nodes, data centres, edge devices or even peer systems. It improve fault tolerance, scalability and availability, which resists centralized failures or insider threats [22]. It also circumscribes the unilateral control over data within the framework of the CSP and increases trust and user privacy [23]. Nonetheless, decentralized systems have difficulty ensuring uniformity of security policies and traditional cryptographic protocols, which are most often optimized to fixed centralized systems. Furthermore, the integrity and consistency of data may be more difficult to support in distributed environments unless powerful synchronization and verification facilities are able to maintain this consistency and integrity.

3.3 Public Key Infrastructure (PKI) and Certificate Authorities (CAs)

A PKI is a system of operations designed to manage, generate, distribute and cancel public-key crypto and electronic certificate. It makes secure electronic communication possible in a number of areas, such as personal email, e-commerce, and online banking. PKI offers critical security services; these services include identification and authentication, data integrity, confidentiality, and non-repudiation, which makes electronic transaction verifiable and secured [24]. It forms the base technology for most of the apps that need secure authentication, such as digital signatures, encrypted messages, smart cards, secure network access, etc.

PKI relies on digital certificates issued by a trusted third party known as Certificate Authorities (CAs) to link a public key with an authenticated identity. These CAs provide the authentication of identity of entities or domains and issue certificates in standardized format e.g. X.509 format which publicly attests the association of the entity and its public key [25]. However, traditional PKI systems are often centralized, which introduces vulnerabilities. For instance, if a CA issues a malicious or compromised certificate, it may go undetected, potentially enabling man-in-the-middle attacks. These limitations highlight the need for more transparent, decentralized, or blockchain-based alternatives to enhance trust and accountability in PKI systems.

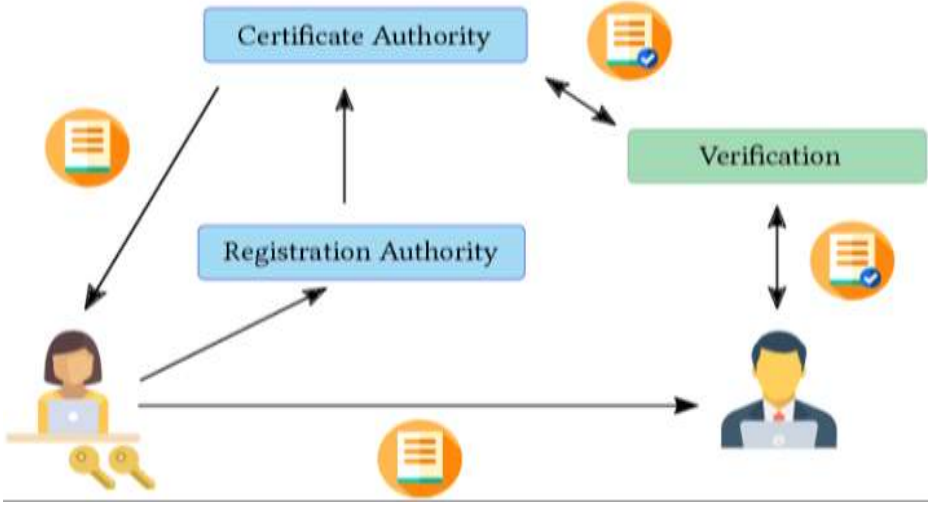

Figure 2: Public Key Infrastructure (PKI)

Figure 2 shows how digital certificates authenticate communication between Alice and Bob obtains a signed certificate via the RA and CA. Alice retrieves and verifies it to ensure Bob's identity, preventing man-in-the-middle attacks, though the process adds time and overhead.

3.4 Blockchain-Based Trust Models

The distributed ledger known as "blockchain" stores information in interconnected, immutable blocks protected by cryptographic hashes. The blocks create an unchangeable chain by referencing one another. Unlike traditional databases, it supports decentralized trust among parties. Its core strengths, built-in cryptography and distributed data management, ensure data integrity, user identity protection, and resistance to tampering[26]. These features make blockchain an effective foundation for secure, decentralised authentication and trust models. A blockchain-based trust and authentication model for secure cross-domain cloud access[27]. A cloud user authenticates with their Home Cloud Service Provider (CSP), which creates and stores an access token on the blockchain. When the user requests a service from a Foreign CSP, the Foreign CSP retrieves a trust certificate from the blockchain to verify the user's credentials (as shown in Figure 3).

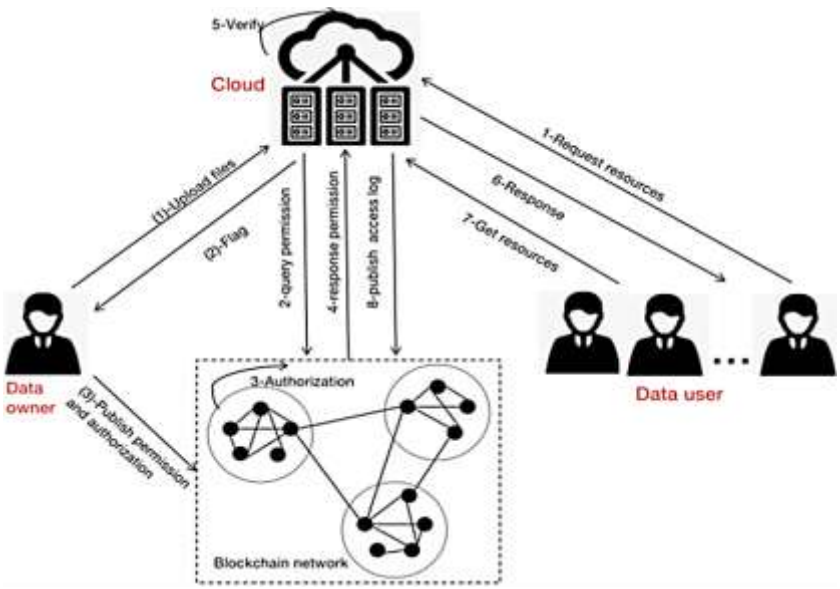

Figure 3: Blockchain-Based Trust Models for Cloud Security

4 INTEGRATION OF ZKPS IN CLOUD ACCESS CONTROL AND AUTHENTICATION

Zero-Knowledge Proofs (ZKPs) are a type of cryptography that enables one party to verify the truth of another's claim without disclosing the underlying evidence. By doing so, sensitive credentials can be securely authenticated and access controlled in cloud environments [28]. There are two primary categories of ZKPs: interactive and non-interactive. While SNARKs and other non-interactive ZKPs (NIZKs) allow for one-time proofs that third parties can verify, interactive ZKPs necessitate numerous exchanges between the prover and verifier. By eliminating the verifier's random challenge, NIZKs prove efficient and secure in a scalable cloud-based authentication system that protects user privacy. Use of ZKPs in cloud access control serves to increase user privacy, minimize dependency on central authorities, and limit the threats of credential abuse. Such capabilities make ZKPs ideal for use in zero-trust architectures and decentralized identity systems on cloud platforms.

4.1 Types of ZKPs

The identified major classes of ZKPs, such as interactive, non-interactive, and succinct proofs, are described together with the functioning details of provably secure authentication and privacy-preserving computations are outlined in this section:

4.1.1 Interactive zero-knowledge proof

The goal of an interactive zero-knowledge proof is to convince the verifier that a given assertion is true by carrying out a series of operations within the context of mathematical probability. In this scenario, the prover can discreetly tell the verifier the truth. There are restrictions on how far an interactive zero-knowledge proof can go. The results of the demonstration cannot be independently verified by anybody other than the verifier. It is also not viable for a dispersed network to handle ZKP due to the recurrent interaction it requires.

4.1.2 Non-Interactive Zero-Knowledge Proof

A non-interactive zero-knowledge proof does not allow the prover and the verifier to communicate in a sequential manner. Since just one message can be sent from the prover to the verifier, channel collisions are reduced. This mechanism is crucial to a wide variety of cryptographic techniques and protocols.

4.1.3 zk-SNARKs and zk-STARKs

Quick verification and concise proofs are made possible by zk-SNARKs, a compact type of non-interactive zero-knowledge proofs. The size of the security parameter and the instance size, rather than the size of the circuit or the witnesses, determine the size and verification time of the proofs produced by zk-SNARKs, in contrast to regular NIZKPs [29]. This makes them efficient for complex applications like private blockchain transactions.

Zero-Knowledge Scalable Transparent Argument of Knowledge (zk-STARKs) is a transparent and quantum-secure alternative to zk-SNARKs. Using hash-based cryptography, they provide off-chain processing with excellent scalability and remove the requirement for a trusted setup. However, zk-STARKs generate larger proofs compared to zk-SNARKs, which may impact efficiency in bandwidth-limited scenarios.

4.1.4 ZKPs in Privacy-preserving Authentication

ZKPs are being used more and more in privacy-preserving authentication methods to make them safer and keep data from getting out [30]. Unlike conventional systems, which require users to disclose sensitive information such as passwords or biometrics, ZKPs enable users to verify their possession of valid credentials without revealing them. This eliminates leak of information and chances of identity theft. In current password-less authentication systems, ZKPs are highly useful when multi-factor authentication mechanisms, like devices, PINs, or biometrics, are used so that identity is proved without leaking any personal information.

4.1.5 Multi-Factor Authentication using ZKPs

Zero-Knowledge Proofs (ZKPs) work with Multi-Factor Authentication (MFA) because they enable users to demonstrate possession of multiple authentication keys. Various combinations of elements based on knowledge (such as passwords), possession (such as tokens or devices), and biometrics fall under this category. One use case is when a user needs to prove they have both the secret key and the registered device at the same time [31]. The strategy can limit the chances of credential exposure yet preserve high authentication in the cloud. Additionally, the distributed systems also make MFA using ZKP particularly appropriate, since untrusted networks are required to perform secure verification [32]. It also provides privacy-preserving access, ensuring sensitive identity attributes remain private during verification.

5 LITERATURE OF REVIEW

This literature review of Cryptographic Trust and Zero-Knowledge Proofs in Secure Authentication Clouds summarizes main trends, empirical data, and technology, and may be used in future research and practical implementation.

Podda *et al.* (2025) investigate the potential impact on legal compatibility of these techniques' accessibility on the European electronic identification scenario and explore the area of potential contradiction between the technological requirements of the digital identity wallet and the concept of data minimisation under GDPR. The second dynamic, in specific settings, was demonstrated by processing cryptographic data to ensure the validity and reliability of electronic attestations of attributes, which shed light on the potential use of ZKPs to strengthen compliance with the law. Regulatory bodies should mandate the implementation of more advanced solutions, like ZKPs, to satisfy the unlikability and non-observability domains. This paper contributes to the privacy-focused research direction of electronic identity management by providing policy and technical advice that has led to compliance with the data minimisation principle. Speeding up the standardisation of such technologies is essential to the protection of user privacy and ensuring a smooth regulatory compliance process in the systems of digital identity [33].

Bhattacharya *et al.* (2024) explores the novel cryptographic approach known as Zero-Knowledge Proofs (ZKP) and how it can be applied to the authentication protocol to enhance privacy. To this purpose, give a comprehensive review of the theoretical underpinnings of ZKPs, zk-SNARKs, and zk-STARKs to show how ZKPs enable credential verification without requiring the user to divulge any personally identifiable information. Almost every current privacy-preserving authentication framework uses a comparative analysis approach to draw parallels and compare and contrast traditional authentication frameworks with ZKP based authentication systems on various metrics, including computing efficiency, scalability, and privacy preservation effectiveness. Investigation of ZKPs indicates that they provide a better model of privacy-protecting authentication with major security loopholes in traditional approaches, and a scalable, efficient process to carry out authentication on a large scale and implement it at scale [34].

Sasikumar and Nagarajan (2024) investigated various cryptography approaches, including DNA, elliptic curve, homomorphic, hybrid, lightweight, and novel approaches. Data security on the cloud is addressed with recommendations after an evaluation of their technique, algorithms, outcomes, uses, and limits. This study presents small approach to secure communication and lightweight cryptography that utilises elliptic curve cryptography (ECC). It is designed for use with resource-constrained, sensitive Internet of Things (IoT) devices. This is an argument make in favor of hybrids combining asymmetric security with symmetric efficiency. Cloud computing is a booming business where different online services are being provided, such as software, computing capabilities, and databases [35].

Roslin Dayana and Shobha Rani (2023) improves the safety of cryptographic RBAC cloud storage systems by reasoning and data protection based on a trust model. Using the user's trust levels as a basis, User Activity Monitoring Agent (UAMA) determines data access rights. Two kinds of user misbehaviour—data leakage and access policy violation—influence a user's trust level, which in turn leads to an upgrade in the access policy. The fact that the user must decode the data before they can access its contents adds an extra layer of protection. The performance of the trust-based RBAC system was assessed using a variety of measures, such as memory consumption, data storage with retrieval time, and fraudulent user detection. The results showed that the suggested approach performed better. With cloud data storage, users may affordably and on-demandly store massive volumes of data [36].

Priyadarshini *et al.* (2022) suggests utilizing Cross-Breed Blowfish in conjunction with MD5 (CBM) to improve the security of health data kept in the CPS cloud. The proposed model utilizes a wireless sensor network, where the transmitting node transfers the data gathered by the network. The fuzzified effective trust-based routing protocol (FET-RP) aims to determine the best path for data transmission. Once the Butter-Ant Optimization (BAO) algorithm is applied, the best course of action is discovered. Through the use of encryption and decryption, the proposed method transfers data in an unencrypted format. Then, a cloud database stores the encrypted data for further security. Through the use of the route-finding algorithm, the data is transferred from one end to the other. The data is encrypted based on its source and destination to ensure optimal performance. examined the proposed method's performance indicators in comparison to those of existing methods, such as RSA, Two Fish, ICC, and FHEA [37].

Tran *et al.* (2021) offer a biometric authentication system driven by artificial intelligence that operates on the binary representation of a biometric instance. The biometric subjects' intraclass and interclass binary strings utilise to train a binary classifier. Classifiers utilised in this examination of fingerprint and iris authentication capabilities include Support Vector Machine and Multi-layer Perceptron Neural Network. The hash value that is produced from the verified biometric text is then used by a Zero-Knowledge-Proof Protocol to ensure confidentiality. A simple approach to making binary strings more discriminative, known as Composite Features Retrieval, could significantly enhance the classifier's identification accuracy. The recommended approach uses UBIRISv1 in tandem with four open-source databases: FVC2002-DB1, FVC2002-DB2, FVC2002-DB3, and FVC2004-DB2 [38].

A comparative summary of the recent studies is given in Table 1 which describes the methods, major conclusions, problems of practical realization, and future perspectives, when moving towards implementation to increase the efficiency of secure cloud authentication methods in various application areas.

Table 1: Literature Summary on Secure Cloud Access Control with Cryptographic Trust Models and Zero-Knowledge Proofs.

Reference	Study on	Approaches	Findings/Insights	Challenges	Future Work

Poddar et al. (2025)	Legal compatibility of ZKPs in EU digital identity systems	Policy and technical analysis; GDPR compliance with ZKPs	ZKPs support data minimization, unlikability, and unobservability in identity systems	Tension between technical requirements and GDPR constraints	Recommend standardizing ZKPs for privacy-compliant digital identity systems
Bhattacharya et al. (2024)	ZKPs in privacy-preserving authentication	Analysis of zk-SNARKs and zk-STARKs from a theoretical and comparative perspective	ZKPs offer stronger privacy, scalability, and computational efficiency than traditional methods	Complexity in implementation and real-world integration	Promote ZKP adoption in scalable, privacy-focused authentication protocols
Sasikumar et al. (2024)	Cryptographic techniques for secure cloud communication	Review of ECC, homomorphic, hybrid, and lightweight cryptography	ECC and lightweight cryptography enhance efficiency and security for cloud and IoT	Limited applicability for resource-constrained environments	Recommend hybrid approaches for combining symmetric and asymmetric cryptography
Roslin Dayana et al. (2023)	Trust model for RBAC-based cloud storage security	Trust degree-based RBAC using user activity monitoring and adaptive access control	Improved detection of policy violations; dynamic trust adjustments enhance security	Managing dynamic trust levels and access revocation	Enhance scalability and real-time trust evaluation mechanisms
Priyadarshini et al. (2022)	Hybrid encryption and trusted routing to strengthen Cyber-Physical System (CPS) security for health data	Protocol for Fuzzified Effective Trust-based Routing using Cross-Breed Blowfish and MD5 (CBM) encryption (FET-RP). For optimal route selection, Butter-Ant Optimization (BAO) - Source and destination data encryption	CBM approach offers enhanced encryption and decryption throughput. Efficient and secure data transmission over wireless sensor networks. Outperforms RSA, Two Fish, ICC, and FHEA in performance metrics	Computational complexity of combined encryption and routing. Balancing between security and transmission efficiency	Improve the scalability and latency of the CBM model in large-scale CPS environments- Integrate with real-time medical monitoring systems
Tran et al. (2021)	Lightweight and privacy-preserving biometric authentication using binary representation	Binary encoding of biometric instances- Classifiers: SVM and MLP Neural Network- Composite Features Retrieval strategy. Zero-Knowledge Proof protocol for privacy	Achieves effective authentication with low computational overhead. Composite Features Retrieval boosts classifier performance- Ensures privacy with ZKP integration	Maintaining high accuracy across diverse biometric datasets. Ensuring robustness against spoofing attacks	Apply method to other biometrics. Explore on-device processing for edge AI implementation

6 CONCLUSION AND FUTURE WORK

Cryptography remains the cornerstone of secure digital infrastructure, ensuring confidentiality, integrity, and authentication across cloud computing, IoT, and distributed systems. With the advent of advanced paradigms such as ZKPs, Access Control as a Service (ACaaS), and blockchain-based trust models, cloud access control is undergoing a significant transformation. These technologies facilitate privacy-preserving, decentralized, and verifiable authentication mechanisms. This study proposes a trust-based cryptographic RBAC framework, reinforced by blockchain to enable secure metadata and key distribution, fair keyword search, and dynamic monitoring of user access behavior using smart contracts. By integrating risk-based, attribute-aware access models, the framework supports context-sensitive decision-making. Additionally, the adoption of AI-driven IAM offers a scalable and intelligent approach to meet the evolving needs of cloud systems. Traditional IAM solutions often lack flexibility and scalability, issues the proposed model seeks to address by emphasizing data privacy, regulatory compliance, and adaptability. However, challenges remain.

Future research should focus on scalable and interoperable ZKP-based authentication protocols for cloud, edge, and IoT. Strengthening blockchain trust frameworks with Public Key Infrastructure (PKI), advancing post-quantum cryptography, and aligning with compliance standards will be crucial to ensure a secure, privacy-respecting, and resilient cloud ecosystem.

REFERENCES

[1] S. Kabade and A. Sharma, "Utilizing Cloud Technologies To Reduce Bottlenecks In Retirement Claim Approvals For Scalable And Efficient Processing," *Int. J. Curr. Sci. (IJCSPUB*, vol. 12, no. 3, 2022.

[2] X. Dong, J. Yu, Y. Luo, Y. Chen, G. Xue, and M. Li, "Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing," *Comput. Secur.*, vol. 42, pp. 151–164, 2014, doi: 10.1016/j.cose.2013.12.002.

[3] V. Shah, "Securing the Cloud of Things : A Comprehensive Analytics of Architecture , Use Cases , and Privacy Risks," vol. 3, no. 4, pp. 158–165, 2023, doi: 10.56472/25832646/JETA-V3I8P118.

[4] A. M. Qadir and N. Varol, "A review paper on cryptography," *7th Int. Symp. Digit. Forensics Secur. ISDFS 2019*, no. June, pp. 1–6, 2019, doi: 10.1109/ISDFS.2019.8757514.

[5] N. Prajapati, "Review of Quantum Computing Advances and their Impact on Modern Cryptographic Security," *Int. J. Innov. Sci. Res. Technol.*, pp. 2023–2035, May 2025, doi: 10.38124/ijisrt/25may501.

[6] B. Soewito and Y. Marcellinus, "IoT security system with modified Zero Knowledge Proof algorithm for authentication," *Egypt. Informatics J.*, vol. 22, no. 3, pp. 269–276, 2021, doi: 10.1016/j.eij.2020.10.001.

[7] V. Prajapati, "Cloud-Based Database Management : Architecture , Security , challenges and solutions," *J. Glob. Res. Electron. Commun.*, vol. 1, no. 1, 2025.

[8] M. A. Shibli, R. Masood, U. Habiba, A. Kanwal, Y. Ghazi, and R. Mumtaz, *Access Control As a Service in Cloud: Challenges, Impact and Strategies*, no. July. 2014. doi: 10.1007/978-1-4471-6452-4_3.

[9] V. Verma, "Big Data and Cloud Databases Revolutionizing Business Intelligence," *TIJER – Int. Res. J.*, vol. 9, no. 1, pp. 48–58, 2022.

[10] S. S. S. Neeli, "Serverless Databases: A Cost-Effective and Scalable Solution," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 7, no. 6, p. 7, 2019.

[11] A. A. Mishra, K. Surve, U. Patidar, and R. K. Rambola, "Effectiveness of confidentiality, integrity and availability in the security of claoud computing: A review," *2018 4th Int. Conf. Comput. Commun. Autom. ICCCA 2018*, no. February, 2018, doi: 10.1109/CCAA.2018.8777537.

[12] M. Hummer, M. Kunz, M. Netter, L. Fuchs, and G. Pernul, "Adaptive identity and access management—contextual data based policies," *Eurasip J. Inf. Secur.*, vol. 2016, no. 1, 2016, doi: 10.1186/s13635-016-0043-2.

[13] O. Obi, S. Dawodu, A. Daraojimba, S. Onwusinkwue, O. Akagha, and I. Ahmad, "REVIEW OF EVOLVING CLOUD COMPUTING PARADIGMS: SECURITY, EFFICIENCY, AND INNOVATIONS," *Comput. Sci. IT Res. J.*, vol. 5, pp. 270–292, 2024, doi: 10.51594/csitrj.v5i2.757.

[14] F. Bassan and M. Rabitti, "From smart legal contracts to contracts on blockchain: An empirical investigation," *Comput. Law Secur. Rev.*, vol. 55, p. 106035, Nov. 2024, doi: 10.1016/j.clsr.2024.106035.

[15] R. Patel and P. Patel, "A Survey on AI-Driven Autonomous Robots for Smart Manufacturing and Industrial Automation," *Tech. Int. J. Eng. Res.*, vol. 9, no. 2, 2022, doi: 10.56975/tijer.v9i2.158819.

[16] M. L. Patel, "Essential Aspects of Security , Privacy and Challenges in Cloud," no. September, pp. 1–6, 2013, doi: 10.13140/RG.2.2.17834.22720.

[17] V. Shah, "Managing Security and Privacy in Cloud Frameworks : A Risk with Compliance Perspective for Enterprises," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 6, pp. 606–618, 2022.

[18] V. Singh, "Reinventing Business with Cloud Integration: The Cost - Effectiveness of Replacing Legacy Applications," *Int. J. Sci. Res.*, vol. 13, no. 8, pp. 1882–1887, 2024.

[19] S. M. Naser, "Cryptography: From the Ancient History To Now, It'S Applications and a New Complete Numerical Model," *Int. J. Math. Stat. Stud.*, vol. 9, no. 3, pp. 11–30, 2021.

[20] Dhruv Patel and Ritesh Tandon, "Cryptographic Trust Models and Zero-Knowledge Proofs for Secure Cloud Access Control and Authentication," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 2, no. 1, pp. 749–758, Dec. 2022, doi: 10.48175/IJARSCT-7744D.

[21] T. Helath, S. Experience, B. Idowu, E. Ogunbodede, and B. Idowu, "Journal of Information Technology Impact," vol. 3, no. 2, pp. 69–76, 2003.

[22] V. M. L. G. Nerella, "Architecting Secure, Automated Multi-Cloud Database Platforms Strategies for Scalable Compliance," *Int. J. Intell. Syst. Appl. Eng.*, vol. 9, no. 1, pp. 128–138, 2021.

[23] Y. Chen, "Comparative Analysis of the Centralized and Decentralized Architecture of Cloud Computing in terms of Privacy Security," *Appl. Comput. Eng.*, vol. 145, no. 1, pp. 51–56, Apr. 2025, doi: 10.54254/2755-2721/2025.21867.

[24] P. Pinchuk, "Maximizing Signal Detection and Improving Radio Frequency Interference Identification in the Search for Radio Technosignatures," *PhD Thesis*, 2021.

[25] A. Akram *et al.*, "A Pilot Study on Survivability of Networking Based on the Mobile Communication Agents," *Int. J. Netw. Secur.*, vol. 23, no. 2, pp. 220–228, 2021, doi: 10.6633/IJNS.202103.

[26] A. Goyal, "Integrating Blockchain for Vendor Coordination and Agile Scrum in Efficient Project Execution," *Int. J. Innov. Sci. Res. Technol.*, vol. 9, no. 12, pp. 1–12, 2024.

[27] N. A. M. Razali, W. N. W. Muhamad, K. K. Ishak, N. J. A. M. Saad, M. Wook, and S. Ramli, "Secure Blockchain-Based Data-Sharing Model and Adoption among Intelligence Communities," *IAENG Int. J. Comput. Sci.*, vol. 48, no. 1, 2021.

[28] G. Maddali, "An Efficient Bio-Inspired Optimization Framework for Scalable Task Scheduling in Cloud Computing Environments," *Int. J. Curr. Eng. Technol.*, vol. 15, no. 3, pp. 229–238, 2025.

[29] L. George and J. J. Kizhakkethottam, "Evolution of Zero-Knowledge Proof (ZKP) and its role in blockchain applications for ensuring data privacy," *Int. J. Eng. Dev. Res.*, vol. 9, no. 1, pp. 165–169, 2012.

[30] A. M. Kadan and E. R. Kirichonok, "Authentication module based on the protocol of zero-knowledge proof," *CEUR Workshop Proc.*, vol. 2914, pp. 365–373, 2021.

[31] Y. L. Maxine, "Analysis of Multi-factor Authentication (MFA) Schemes in Zero Trust Architecture (ZTA): Current State , Challenges , and Future Trends," vol. 186, no. 57, pp. 30–36, 2024.

[32] V. M. L. G. Nerella, "Automated Compliance Enforcement in Multi-Cloud Database Environments: A Comparative Study of Azure Purview, AWS Macie, and GCP DLP," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 11, no. 4, pp. 270–283, 2025.

[33] E. Podda, P. Hölzmer, A. Amard, J. Sedlmeir, and G. Fridgen, "The impact of zero-knowledge proofs on data minimisation compliance of digital identity wallets," *Internet Policy Rev.*, vol. 14, no. 3, Jul. 2025, doi: 10.14763/2025.3.2019.

[34] S. Bhattacharya, D. Seth, S. Panyam, and P. Gangrade, "Enhancing Digital Privacy: The Application of Zero-Knowledge Proofs in Authentication Systems," *Int. J. Comput. Trends Technol.*, vol. 72, no. 4, pp. 34–41, Apr. 2024, doi: 10.14445/22312803/IJCTT-V72I4P104.

[35] K. Sasikumar and S. Nagarajan, "Comprehensive Review and Analysis of Cryptography Techniques in Cloud Computing," *IEEE Access*, vol. 12, pp. 52325–52351, 2024, doi: 10.1109/ACCESS.2024.3385449.

[36] K. Roslin Dayana and P. Shobha Rani, "Trust aware cryptographic role based access control scheme for secure cloud data storage," *Automatika*, vol. 64, no. 4, pp. 1072–1079, Oct. 2023, doi: 10.1080/00051144.2023.2243144.

[37] R. Priyadarshini, A. Quadir Md, N. Rajendran, V. Neelanarayanan, and H. Sabireen, "An enhanced encryption-based security framework in the CPS Cloud," *J. Cloud Comput.*, vol. 11, no. 1, p. 64, Oct. 2022, doi: 10.1186/s13677-022-00336-z.

[38] Q. N. Tran, B. P. Turnbull, M. Wang, and J. Hu, "A Privacy-Preserving Biometric Authentication System With Binary Classification in a Zero Knowledge Proof Protocol," *IEEE Open J. Comput. Soc.*, vol. 3, pp. 1–10, 2021, doi: 10.1109/OJCS.2021.3138332.

