IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, December 2022

Cryptographic Trust Models and Zero-Knowledge Proofs for Secure Cloud Access Control and Authentication

Dhruv Patel and Ritesh Tandon
Independent Researcher
dp270894@gmail.com and ritz10don@gmail.com

Abstract: *Cryptography is one of the most important approaches to keep digital communication in lock and key and therefore guarantees the privacy, integrity and authenticity of the data by means of complex coding. Cryptographic techniques have arisen centuries ago and the old techniques have continued to evolve as today's challenges are cloud computing, data storage and retrieval as well as authenticated users. With the widespread spread of cloud environments, trust-enabling systems with cutting-edge technologies such as Zero Knowledge Proofs and blockchain emerged to increase privacy and security. By examining the notion of trust localization, this study draws attention to a use of Gateways as access control points to sensitive information reducing the dependence on the central cloud infrastructures. Additionally, source authentication and authorization provided by Acaras and PKI is studied regarding their integration and effectiveness. The research examines the current challenges in cryptographic security and current findings of cryptographic security and investigates what the future of cryptographic security to build trust and security in modern digital systems..*

Keywords: Cryptography, Zero-Knowledge Proofs (ZKPs), Cloud Security, Public Key Infrastructure (PKI), Access Control as a Service (ACaaS)

I. INTRODUCTION

Cloud computing [1], in recent years, has revolutionized the way in which data is stored as well as the way in which data can be computed, providing a scalable and inexpensive infrastructure for outsourcing this service. Virtualization, service-oriented computing, and other emerging technologies make available computing power from large resource bases that permits users to access these resources with little if any local management. Cloud services come in three main types: IaaS, PaaS, and SaaS. PaaS, SaaS, and IaaS include services like Google App Engine, Microsoft Azure, and Amazon EC2. Users may rent, manage, and use computing equipment with ease thanks to their pay-as-you-go concept.

Although cloud computing offers an attractive suite of benefits, it brings about serious privacy and security problems. Outsourcing of the data and computation sometimes relieves enterprises from the control of digital assets, and then the questions on their data confidentiality, integrity, and governance arise. Cloud users are at the mercy of various security threats and malicious attacks because of the lack of direct oversight [2]. Therefore, due to the need for access control and authentication in the cloud, these mechanisms have become important to establish secure and trustworthy ways.

Secure communication and data confidentiality is ensured by cryptography is long history [3]. Cryptography is one of the sophisticated fields that historically rooted in secret writing techniques and developed from 2000 B.C. Nowadays, it carries out an important role in protecting digital communication and enforcing security policies throughout distributed systems.

The technique is Zero Knowledge Proofs (ZKPs) [4], which is a really potent cryptography instrument, used more and more times in modern authentication systems. A ZKP lets a prover show that a statement is accurate without providing the checker with any details about its foundation. A zero-knowledge protocol (ZKP) is an authenticated way for entities to show their identities or rights without giving out sensitive credentials. It was first described in the book "How to Explain Zero Knowledge Protocols to Your Children." It comes in particularly handy in the cloud, where one needs to prevent information exposure.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, December 2022

This has led to the development of cryptographic trust models in distributed cloud environments to further increase the security [5]. These models build structured methods for the estimation of the trustworthiness of users and service providers when semi-trusted or decentralized. Trust models integrated with ZKPs provide a robust path for the creation of authentication and control mechanisms to provide users with a way to access cloud services securely but preserving their privacy.

In addition, ACaaS has emerged as a cloud-based solution for authenticating and authorizing in the cloud [6]. ACaaS decouples the access control decisions from the applications and externalizes them to a trusted third-party provider, thus reducing the complexity of developing applications and facilitating the seamless integration between multiple services. This allows users to have single sign-on capabilities using the authentication token and authorization claim while leveraging central and scalable access control management capabilities.

A. Structure of the Paper

This study investigates zero-knowledge proofs and cryptographic trust models for safe cloud access and authentication. Key cloud security issues are outlined in Section II, trust models and ZKPs are covered in Sections III–IV, related work is reviewed in Section V, and future approaches are discussed in Section VI.

II. KEY CONSIDERATIONS FOR SECURE CLOUD COMPUTING

The primary characteristic of the cloud computing environment is the protection of data and resources. Cloud security acts as a barrier that protects all of the important data, software, and technology stored in the cloud. Because security concerns are the same whether you're using a public, private, or hybrid cloud system, this is crucial. Some businesses and study groups are hesitant to fully adopt cloud computing because they are concerned about their data security. A security threat can affect both on-premises and cloud-based IT platforms. Because of this, cloud security is necessary to protect data and networks properly and to quickly find and deal with any strange or odd events. Cloud security methods that work must always change to keep up with new hackers. Here are some of the most important problems with cloud computing. Some of them cause services to be delayed, while others can be fixed with care and attention:

- **Security and Privacy:** These problems can be fixed by keeping the data inside the company but letting people use it in the cloud, for example [7][8]. But for this to happen, the security between the organization and the cloud needs to be strong. A hybrid cloud could allow this kind of deployment.
- **Lack of Standards:** Most clouds will not be able to work with each other, even though their interfaces are written down. This is because there are no guidelines for these interfaces. It is working on Guidelines on cloud computing and the Open Cloud Computing Interface of the Open Grid Forum and best practices through the Open Cloud Consortium. It's too early to tell if these groups' results will meet the needs of the people putting the services in place, but they will need time to develop [9].
- **Continuously Evolving:** The needs of users and the needs for connections, networking, and storage are always changing. This means that a cloud, especially a public one, doesn't stay the same and is always changing.
- **Compliance Concerns:** These problems usually lead to the use of a hybrid cloud, where one cloud stores data that is specific to the organization.

A. Data Confidentiality, Integrity, and Availability

Confidentiality refers to safeguarding the data the information from unauthorized clients. There may be some users or clients who might want unnecessary access to the data of other users and may use it for some illegal work. There is possibility that the person may change details of others without authority. Other than data the virtual machine image, virtual machine manager and others also has confidentiality requirements.

Confidentiality means keeping data and information safe from people who aren't supposed to have access to them. However, there may be users or clients who want to see other users' data without a good reason and may use it to do bad things [10]. The person could change information about other people without permission. Besides data, the virtual machine picture, the virtual machine manager, and other things must also be kept secret.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, December 2022

Integrity means that the info is guaranteed to be real. Third parties who haven't been given permission to do so shouldn't be able to change the data. Cloud-based services can be reached through the internet, which makes them very vulnerable to attacks that could damage the data. The data must be kept consistent, correct, and reliable throughout its entire lifetime. Most of the time, making sure there are backups and copies of the data in case it gets lost or damaged is the best way to make sure it stays safe.

Availability is the third important basic part of data protection. This part is about how well the cloud-based apps work when they're supposed to [11]. When a client asks for data, not having it can cause huge loses that can't be recovered. Availability is among the key components of information security. The quality and safety of the data can't be compromised, so the SLA lists the promises the service has made about being available and responding quickly to requests.

B. Identity and Access Management (IAM) Issues

One of the biggest security problems companies face today is making sure staff can access sensitive data and applications in a smart way [12]. Large companies usually control the entry rights of millions of users to thousands of IT resources. Employees get too many access rights over time because user management isn't done well or is application-specific. Because of this, most people are overprivileged, which means they have more rights than they need to do their jobs. On the other hand, rules and guidelines for an organization are hard to enforce in a decentralized setting. Because of this, businesses set up an identity and access management (IAM) system that works across the whole company so that digital accounts can be managed centrally. IAM systems are made up of three parts: policies, technologies, and routines.

Three key components make up Identity and Access Management (IAM) systems: Infrastructure-stored IAM data, tool-supported functionality for job automation and user management, and policies that establish guidelines for the overall management of the IAMs. Figure 1 shows the Identity and Access Management.

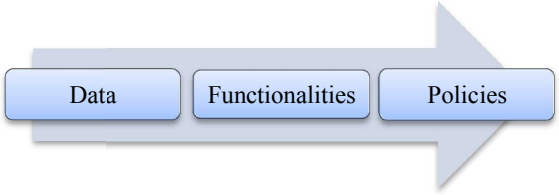

Figure 1: IAM Issues

- **Data:** The IAMS typically loads the required data from associated applications on a regular basis [13]. Those can be business tools with their own user management, like the Microsoft Active Directory or SAP systems.
- **Functionalities:** A system's operation and automatic services are controlled by its Identity and Access Management functions. Within this group are tools for managing users, controlling access, handling and syncing data, and setting up new users. Access management features verify and allow people, while user management handles the identity lifecycle. Working with data means combining information from different programs and sending and receiving data in a uniform way.
- **Policies:** IAMS's data and functions are both controlled by rules that tell them how to work. In a general sense, describe different types of policies and the areas where they are most useful. Explains three kinds of policies: policies for authorization, policies for obligation, and policies for delegation. Similarly, divide policies into three groups: security policies, IAM policies, and process policies.

III. CRYPTOGRAPHIC TRUST MODELS FOR CLOUD SECURITY

Graphene, which means "writing," and cryptos, which means "hidden," are the Greek terms from which cryptography is derived." So, cryptography means both "hidden" and "writing" [14]. Cryptography is usually the act of communicating with someone or a group of individuals in a way that is private and unreadable by others. As soon as people started living in different groups, or tribes, they all thought they were stronger than the others and should rule over the other tribes. But they want to talk to each other in a safe and private way, which is why primary cryptography was created and is shown in Figure 2.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, December 2022

Cryptography has grown into an important way to build trust in IoT networks [15][11][16]. A good example of this is PKI-based trust models, which use digital certificates like X.509 certificates to build trust. To use these models to figure out trust measures, it will need full cryptographic information, though. PKI or X.509 certificate-based trust models don't always take into account what organizations want.

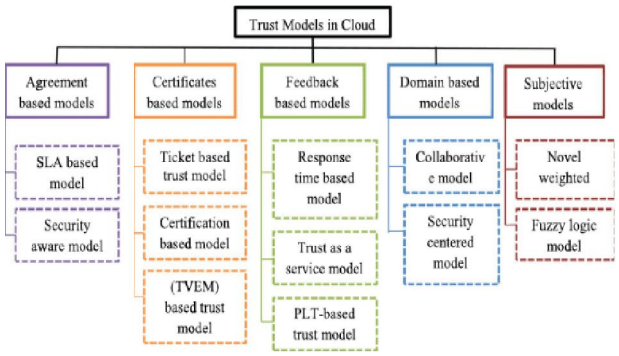

Figure 2: Trust models in cloud computing

A. Definition and Importance of Trust Models

Trust models are often linked to public key systems, where the sharing and ownership of certain information affects how people behave when they are talking to each other [17][18]. Asymmetric encryption, in particular, makes it possible to link faith with the knowledge that public information is linked to a person. Trust models are mostly concerned with these steps that connect the public key to the person or thing that it belongs to [19]. PKI with a root Certificate Authority and the PGP Trust Model are two well-known trust models. The PGP Trust Model is also known as a "web of trust."

Importance of Trust Models in Cryptography for Cloud Security The following highlights the significance of trust models in cloud security cryptography:

- **Establishing Trust Between Cloud Users and Providers:** Trust models help define the security expectations between CSPs and users. Since cloud users store their data on third-party infrastructure, cryptographic trust models ensure that data remains protected even when the underlying infrastructure is not fully under their control [20].
- **Enhancing Data Confidentiality and Integrity:** Cryptographic trust models use encryption, digital signatures, and hashing techniques to prevent unauthorized access and tampering. For instance, Public Key Infrastructure (PKI) helps authenticate entities, ensuring that data integrity is maintained and only authorized users can decrypt sensitive information.
- **Zero-Knowledge Proofs (ZKPs) for Privacy:** Preserving Authentication: ZKPs allow authentication without disclosing private information, which lowers the risks that come with data disclosure. When it comes to cloud security, ZKPs let users show who they are or what access they have without giving out their passwords or credentials. This lowers the risk of credential theft.
- **Public Key Infrastructure (PKI) for Authentication:** PKI trust models use digital certificates to set up a safe communication system. This guarantees that cloud resources can only be accessed by permitted people and devices. Cloud-based applications that use PKI-based authentication are immune to phishing and man-in-the-middle assaults.

B. Public Key Infrastructure (PKI) and Certificate Authorities (CAs)

A framework for making and handling digital certificates and public key encryption, Figure 3, is called a PKI [21]. For many web activities, like private emailing, shopping online, and banking on the internet, the main goal is to help keep electronic information safe during transmission. Because of the structure, digital certificates and public-key encryption can be made, used, stored, managed, distributed, and revoked. One way to set up trusted contact on a network is with public key infrastructure (PKI) [22].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, December 2022

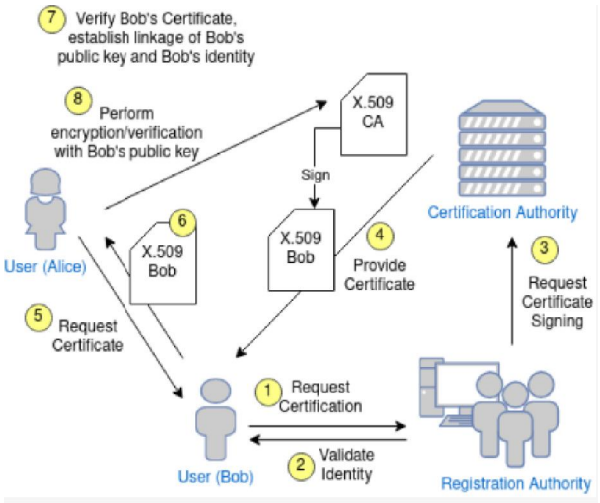

Figure 3: Public Key Infrastructure

This field has grown to become the basis for safe data transfer and internet safety. It is the combination of identification and authentication, data integrity, privacy, and technical non-repudiation that makes any kind of electronic exchange safe and impossible to break.

The main part of many programs that need safe and solid authentication is a public key infrastructure (PKI) [23]. This includes digital signatures and encryption for email, smart cards, and network links. A PKI makes sure that an entity is linked to its public key, usually by using key servers that are kept safe by certificate authorities (CA) [24]. These groups give a domain or person a certificate that openly and verifiably connects that thing to a certain key. X.509 is a common format for these kinds of certificates. The old way of setting up PKI is centralized and has some issues, like harmful certificates that can go unnoticed and let attackers act as a go-between.

C. Blockchain-Based Trust Models for Cloud Security

The blockchain is a new kind of store [25][26] In contrast to SQL or NoSQL databases, blockchain can be shared directly by a group of people who believe each other and people who don't. A distributed database known as a blockchain stores a list of ordered entries, or blocks, that are constantly expanding in an unalterable manner. Every block has a timestamp that is connected to the block that comes before it. The parent block or the block before it has the hash number that is used to connect the blocks.

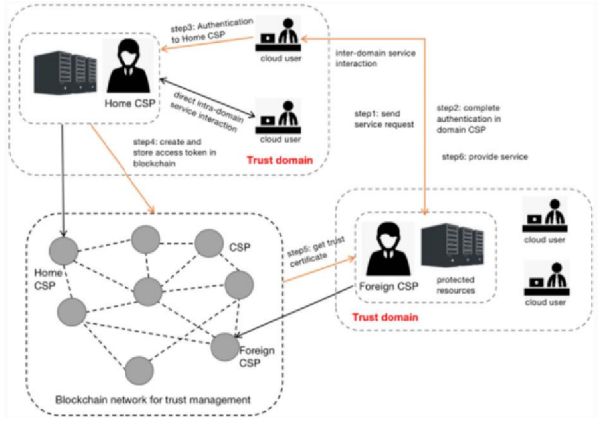

Figure 4: Blockchain-Based Trust Models for Cloud Security

As shown in Figure 4, a block can go through the whole blockchain and find every transaction that happened through its parent block [27]. The birth block is the first block and does not have a parent. There are two major things that make blockchain different from other scalable databases: i) it uses cryptography by design and ii) it manages data in a

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, December 2022

distributed way. When cryptography is used to protect user privacy, the stability of the ledger, and the authenticity of data, this is called "cryptography by design." Depending on the system, the cryptography of each block is different. The hashing method is used to make sure that blocks are well-formed so that they can keep their security of not being changed and becoming almost impossible to break.

IV. ZERO-KNOWLEDGE PROOFS (ZKPS) IN CLOUD AUTHENTICATION

ZKPs, or zero-knowledge proofs, are techniques for verifying statements without disclosing the details. With this approach, a "prover" provides a "verifier" with evidence to support their assertion. The "verifier" then verifies the correctness of the evidence without learning anything more. [28]. ZKPs can be interactive, which means that more than one contact is needed to get close to certainty, or non-interactive, which allows for simultaneous verification of the evidence. Snark is one instance of a non-interactive ZKP. It's brief, space-efficient, and allows for to utilize of a computation's outcome as a statement. Interactive and non-interactive ZKPs vary primarily in that the former employ a common reference value in place of the verifier's random challenges. This makes it possible to send the proof to other people.

A. Types of ZKPs (Interactive vs. Non-Interactive)

Different kinds of ZKPs (interactive and non-interactive). Each kind of ZKP is different:

- Interactive zero-knowledge proof
- Non-interactive zero-knowledge proof

Interactive Zero-Knowledge Proof

Interactive zero-knowledge proofs use a sequence of events designed to persuade the verifier of a certain fact by using mathematical probability. Without alerting the checker, the prover can demonstrate the fact in this situation. It can't apply interactive zero-knowledge proof everywhere [29][30]. Other than the verifier, this means that no one else can check the result of the demonstration. Also, ZKP can't work on a spread network because it requires a lot of repeated interactions.

Non-Interactive Zero-Knowledge Proof:

The prover and the verifier do not communicate in a non-interactive zero-knowledge proof [31]. In this scenario, the prover will only communicate with the checker once, preventing channel collisions. A lot of different kinds of cryptographic protocols and encryption methods are built on this system [32].

B. ZKPs in Password Less Authentication

Single sign-on and two-factor authentication are two technologies that are commonly used to protect web apps in the real world [33]. Often confused, a new trend called "password less web authentication" has been getting a lot of attention lately.

Authentication methods that don't need a password in the usual sense are very similar. To use a multi-factor authenticator, either a PIN (something you know) or a biometric (what you have) is needed. In Multifactor Authenticator, multiple verification methods are used without stacking one-factor authenticators on top of each other.

Using biometrics, encryption, and password-less authentication methods like FIDO2 standard and hardware tokens can successfully stop credential theft and phishing attacks, making the authentication process easier and safer for users.

V. LITERATURE REVIEW

This section reviews the research on zero-knowledge proofs and cryptographic trust models for secure cloud access control.

Chia et al. (2021) show off a practical hybrid PKI that can establish confidence with the current certificate authority while generating new identity-based cryptographic keys for verification. they offer a set of tools that can be used to create and activate these keys in both identity-based and external settings. their custom naming system, which works for

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, December 2022

a few situations right now, manages key revocation. By combining Compared to earlier hybrid PKI–IBC systems, their implementation of Identity-based cryptography (IBC) in X.509 standards improves compatibility [22].

Ren et al. (2021) one of the most crucial aspects of cloud storage security is access control, which lets people who are supposed to be there get in while discouraging people who aren't supposed to be there. The most up-to-date digital access control systems use either identity-based or attribute-based encryption. They usually take on the problem of key exchange, which makes it impossible to find the pirate. As a result of the release of cryptographic industry standards, types of cryptographic methods that follow these standards can be used more effectively in industry. This study proposes SM9-based TA2C) to help find and hold pirates responsible [34].

Ning et al. (2021) A new cloud service called secure cloud storage aims to safeguard the privacy of data that is outsourced while granting cloud customers who do not physically own their data unrestricted access to it. One of the most hopeful methods that can be used to protect the guarantee of the service is CP-ABE. There is, however, a chance that someone will misuse their access credentials (i.e., decryption rights) if they use CP-ABE because it has a "all-or-nothing" decoding feature [35].

Galis et al. (2021) discuss two new ideas for creating secure keys in symmetric systems. Both ideas enable the symmetric cryptographic systems' decentralized key generation, which eliminates the requirement for a third party to be trusted. Systems built on these principles create cryptographic keys at random that are highly effective at maintaining confidentiality. Based on security, keys made by various ideas are categorized into various security classes [36].

Puggioni et al. (2020) a lot of IoT gadgets are being used all over the world, and many of them are very vulnerable. So, making sure IoT devices have regular software changes is very important for keeping them safe. When manufacturers try to update the software on IoT products, they face two main problems: 1) the potential for expansion of the present client-server paradigm; and 2) the security of distributed updates, which is hampered by the processing capacity of the devices and their deficiency in fundamental cryptographic operations. Because of these problems, we'd like to suggest Crowd Patching, a decentralized blockchain-based protocol that lets software makers give self-interested distributors the job of delivering software updates in return for cryptocurrency [37].

Chowdhury et al. (2019) suggest a trust model to help people who don't trust each other get along. After that, they show a model of a reference system that is based on the confidence model created and gives people a reason to securely exchange their health information via a data marketplace. Researchers will be able to get big sets of data for little money if they can get people to share their real-time health data [38].

Table I summarizes key topics, focus areas, challenges, and insights from recent research on Cryptographic Trust Models and Proofs of Zero-Knowledge for Safe Cloud Access Management

Table 1: Literature review on Cryptographic Trust Models and Zero-Knowledge Proofs for Secure Cloud Access Control

Reference	Key Topic	Challenges	Focus Area	Findings/Insights	Future Work
Chia et al. (2021)[22]	Hybrid PKI with Identity-Based Cryptography	Key revocation, interoperability, bootstrapping trust with existing CAs	Identity-Based Cryptography, Hybrid PKI	Introduced a practical hybrid PKI that issues IBC keys and supports X.509 standards for better integration.	Improve the scalability of the naming system for key management and extend compatibility with broader PKI infrastructures
Ren et al. (2021)[34]	Access Control using SM9-based Cryptography	Key exchange vulnerability, inability to trace misuse	Traceable Access Control in Cloud Storage	Proposed TA2C system to trace and hold malicious actors accountable using SM9-based encryption.	Extend traceability mechanisms to multi-cloud environments and investigate performance optimization of SM9-based schemes.
Ning et al.	Secure Cloud	Misuse of access	Attribute-	Highlighted privacy	Develop fine-grained

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, December 2022

(2021)[35]	Storage with CP-ABE	credentials due to all-or-nothing decryption property	Based Ciphertext-Policy Encryption	issues and potential misuse in CP-ABE-based secure cloud storage.	revocation techniques and explore hybrid CP-ABE models with traceability support.
Galis et al. (2021)[36]	Symmetric Cryptographic Key Generation	Trusted third-party requirement for symmetric key generation	Decentralized Key Management	Introduced two new models for decentralized symmetric key generation with security classification.	Analyze scalability and efficiency in large distributed environments; formalize security proofs for each key class.
Puggioni et al. (2020)[37]	IoT Security Updates via Blockchain	Scalability of client-server model, device limitations, and cryptographic resource constraints	Blockchain-based IoT Software Update Distribution	Proposed "Crowd Patching" – a decentralized, incentive-driven update system using blockchain and crypto.	Evaluate protocol robustness against adversarial nodes and implement lightweight cryptographic primitives for resource-constrained devices.
Chowdhury et al. (2019)[38]	Trust Models for Data Sharing	Lack of trust between parties for health data sharing	Data Marketplace, Trust Management	Developed a reference trust model encouraging secure sharing of personal health data in a data marketplace.	Integrate zero-knowledge proofs to enhance privacy and trust, and validate the model through real-world healthcare data-sharing scenarios.

VI. CONCLUSION AND FUTURE WORK

Cryptography, with its origins rooted in ancient secret writing, has evolved into a cornerstone of modern digital security. In areas like cloud computing, the IoT, and other Internet-based applications, it is essential to maintain data confidentiality, integrity, and authentication. Trust mechanisms have been greatly improved by emerging security technologies such as ZKP, ACaaS, and blockchain-based trust models by enabling decentralized and efficient authentication. Nevertheless, persistent concerns related to privacy, identity management, and regulatory compliance underscore the continued need for innovation in cryptographic security system design.

Looking forward, the next decade of cryptographic research should emphasize the advancement of privacy-preserving authentication mechanisms, particularly ZKPs, to further strengthen security in cloud and IoT ecosystems. Integrating blockchain trust models with Public Key Infrastructure (PKI) may offer a scalable and decentralized solution for identity authentication. Moreover, the development of standardized protocols for ACaaS and the formulation of post-quantum cryptographic solutions will be critical in addressing threats posed by quantum computing. Equally essential will be the refinement of cryptographic systems that effectively balance regulatory compliance with robust data protection, thereby fostering greater trust and adoption of cloud-based security frameworks.

Future studies should concentrate on improving privacy-preserving authentication techniques, including Zero-Knowledge Proofs (ZKPs), for safe cloud and Internet of Things settings. Expanding the use of Public Key Infrastructure (PKI) in conjunction with blockchain-based trust models can provide decentralized and scalable identity verification. It is also crucial to build post-quantum cryptography approaches and standardized Access Control as a Service (ACaaS) protocols. The development of cryptographic frameworks that guarantee legal compliance while preserving robust data security should also be a goal in order to promote wider usage of cloud security solutions.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, December 2022

REFERENCES

[1] N. Fotiou, A. Machas, G. C. Polyzos, and G. Xylomenos, "Access control as a service for the Cloud," J. Internet Serv. Appl., vol. 6, no. 1, 2015, doi: 10.1186/s13174-015-0026-4.
[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] A. M. Qadir and N. Varol, "A Review Paper on Cryptography," in 2019 7th International Symposium on Digital Forensics and Security (ISDFS), IEEE, Jun. 2019, pp. 1–6. doi: 10.1109/ISDFS.2019.8757514.
[4] 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.
[5] S. Garg, "Predictive Analytics and Auto Remediation using Artificial Inteligence and Machine learning in Cloud Computing Operations," Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci., vol. 7, no. 2, 2019.
[6] W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya, "Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions," J. Cloud Comput., 2021, doi: 10.1186/s13677-021-00247-5.
[7] M. L. Patel, "Essential Aspects of Security, Privacy and Challenges in Cloud," GIT-Journal Eng. Technol., vol. Sixth, pp. 1–6, 2013, doi: 10.13140/RG.2.2.17834.22720.
[8] V. Singh, "Lessons Learned from Large-Scale Oracle Fusion Cloud Data Migrations," Int. J. Sci. Res., vol. 10, no. 10, pp. 1662–1666, 2021.
[9] G. Modalavalasa, "The Role of DevOps in Streamlining Software Delivery: Key Practices for Seamless CI/CD," Int. J. Adv. Res. Sci. Commun. Technol., vol. 1, no. 12, pp. 258–267, Jan. 2021, doi: 10.48175/IJARSCT-8978C.
[10] A. A. Mishra, K. Surve, U. Patidar, and R. K. Rambola, "Effectiveness of Confidentiality, Integrity and Availability in the Security of Cloud Computing: A Review," in 2018 4th International Conference on Computing Communication and Automation (ICCCA), IEEE, Dec. 2018, pp. 1–5. doi: 10.1109/CCAA.2018.8777537.
[11] Abhishek and P. Khare, "Cloud Security Challenges: Implementing Best Practices for Secure SaaS Application Development," Int. J. Curr. Eng. Technol., vol. 11, no. 06, pp. 669–676, Nov. 2021, doi: 10.14741/ijcet/v.11.6.11.
[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] M. Hummer, M. Kunz, M. Netter, L. Fuchs, and G. Pernul, "Advanced identity and access policy management using contextual data," Proc. - 10th Int. Conf. Availability, Reliab. Secur. ARES 2015, no. August, pp. 40–49, 2015, doi: 10.1109/ARES.2015.40.
[14] 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.
[15] K. M. R. Seetharaman, "Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges, and Opportunities," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 2, pp. 499–508, Mar. 2021, doi: 10.48175/IJARSCT-6268B.
[16] Ş. Bahtiyar, "A hybrid trust-modeling approach for IoaT security," Electrica, vol. 20, no. 1, pp. 86–96, 2020, doi: 10.5152/ELECTRICA.2020.19090.
[17] T. Helath, S. Experience, B. Idowu, E. Ogunbodede, and B. Idowu, "Journal of Information Technology Impact," vol. 3, no. 2, pp. 69–76, 2003.
[18] A. Goyal, "Enhancing Engineering Project Efficiency through Cross-Functional Collaboration and IoT Integration," Int. J. Res. Anal. Rev., vol. 8, no. 4, pp. 396–402, 2021.
[19] A. Kanwal, R. Masood, M. A. Shibli, and R. Mumtaz, "Taxonomy for trust models in cloud computing," Comput. J., vol. 58, no. 4, pp. 601–626, 2015, doi: 10.1093/comjnl/bxu138.
[20] A. Kushwaha, P. Pathak, and S. Gupta, "Review of optimize load balancing algorithms in cloud," Int. J. Distrib. Cloud Comput., vol. 4, no. 2, pp. 1–9, 2016.
[21] P. Pinchuk, "Maximizing Signal Detection and Improving Radio Frequency Interference Identification in the Search for Radio Technosignatures," PhD Thesis, 2021.
[22] J. Chia, S. H. Heng, J. J. Chin, S. Y. Tan, and W. C. Yau, "An implementation suite for a hybrid public key infrastructure," Symmetry (Basel)., vol. 13, no. 8, pp. 1–28, 2021, doi: 10.3390/sym13081535.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 6.252
Volume 2, Issue 1, December 2022

[23] 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.
[24] S. Shah and M. Shah, "Deep Reinforcement Learning for Scalable Task Scheduling in Serverless Computing," Int. Res. J. Mod. Eng. Technol. Sci., vol. 3, no. 12, Jan. 2021, doi: 10.56726/IRJMETS17782.
[25] J. Thomas, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," Int. J. Res. Anal. Rev., vol. 8, no. 3, pp. 874–878, 2021.
[26] 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.
[27] D. D. Rao, A. A. Waoo, M. P. Singh, and F. Paul, "Breaking Down Barriers: Scalability and Performance Issues in Blockchain-Based Identity Platforms Achieving Scalable and High-Performance Blockchain-Based Identity Systems," 2021.
[28] A. Gogineni, "Novel Scheduling Algorithms for Efficient Deployment of Mapreduce Applications in Heterogeneous Computing," Int. Res. J. Eng. Technol., vol. 4, no. 11, 2017.
[29] A. V. Hazarika, G. J. S. R. Ram, and E. Jain, "Performance Comparision of Hadoop and Spark Engine," in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), IEEE, Feb. 2017, pp. 671–674. doi: 10.1109/I-SMAC.2017.8058263.
[30] S. S. S. Neeli, "Serverless Databases : A Cost-Effective and Scalable Solution," IJIRMPS, vol. 7, no. 6, 2019.
[31] 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.
[32] A. Gogineni, "Automated Deployment and Rollback Strategies for Docker Containers in Continuous Integration/Continuous Deployment (CI/CD) Pipelines," Int. J. Multidiscip. Res. Growth Eval., vol. 1, no. 5, 2020.
[33] 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.
[34] K. Ren, P. Jiang, K. Gai, L. Zhu, and J. Huang, "SM9-based Traceable and Accountable Access Control for Secure Multi-user Cloud Storage," in Proceedings - 2021 IEEE 6th International Conference on Smart Cloud, SmartCloud 2021, 2021. doi: 10.1109/SmartCloud52277.2021.00010.
[35] J. Ning, Z. Cao, X. Dong, K. Liang, L. Wei, and K. K. R. Choo, "CryptCloud: Secure and Expressive Data Access Control for Cloud Storage," IEEE Trans. Serv. Comput., 2021, doi: 10.1109/TSC.2018.2791538.
[36] M. Galis, T. Unkasevic, M. Milosavljevic, Z. Banjac, and P. Milosav, "Modern techniques for decentralized key establishment in symmetric cryptographic systems," in 2021 29th Telecommunications Forum, TELFOR 2021 - Proceedings, 2021. doi: 10.1109/TELFOR52709.2021.9653401.
[37] E. Puggioni, A. Shaghaghi, R. Doss, and S. S. Kanhere, "Towards Decentralized IoT Updates Delivery Leveraging Blockchain and Zero-Knowledge Proofs," in 2020 IEEE 19th International Symposium on Network Computing and Applications, NCA 2020, 2020. doi: 10.1109/NCA51143.2020.9306689.
[38] M. J. M. Chowdhury et al., "Trust modeling for blockchain-based wearable data market," in Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom, 2019. doi: 10.1109/CloudCom.2019.00070.