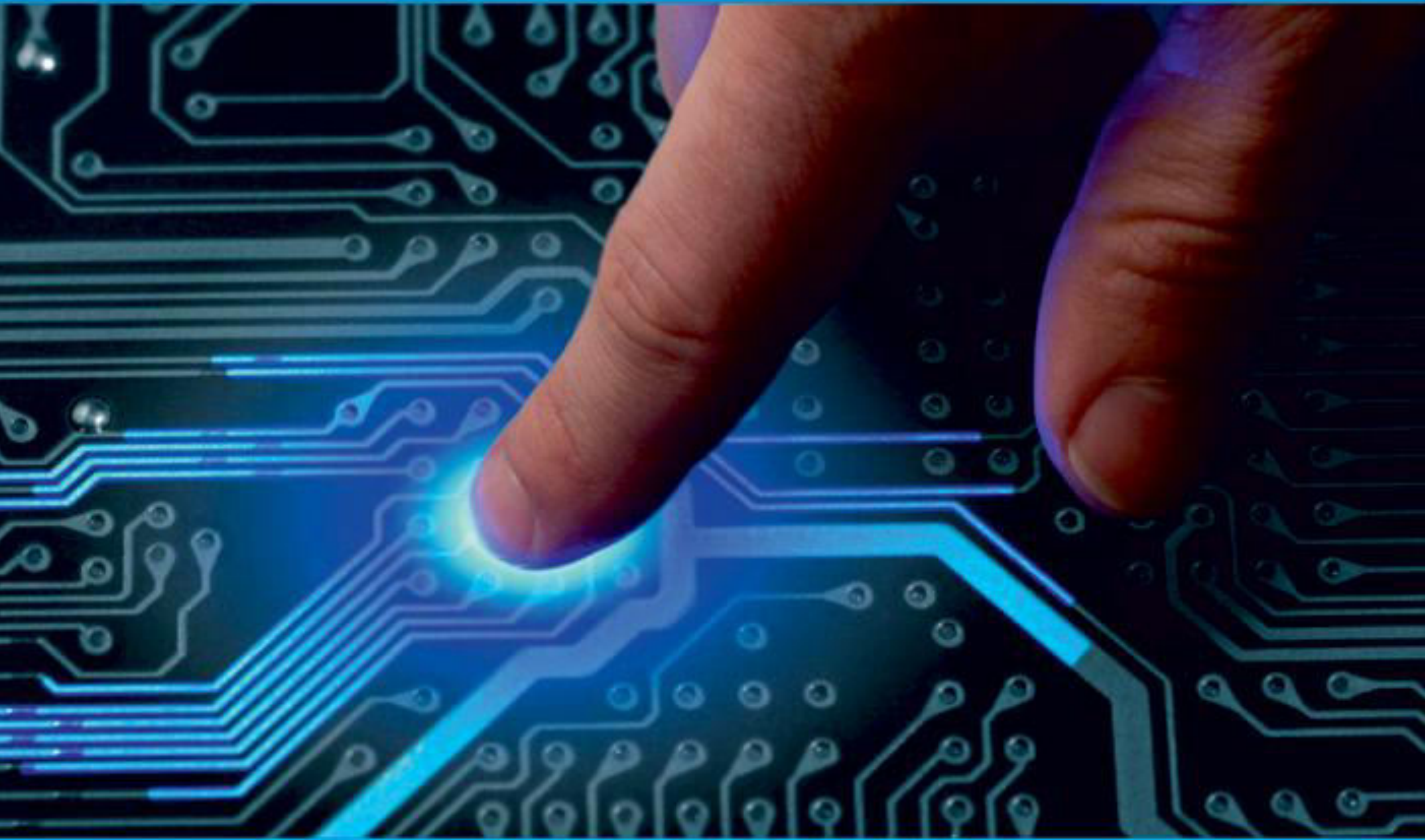
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907020 |

# Fast Secure and Anonymous Key Agreement

**Shifa Anjum A, Dr. Mohammed Tajuddin**

PG Student, Dept. of CSE, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India

Associate Professor, Dept. of CSE, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India

**ABSTRACT**: Cloud computing has become the fastest growing technology in the IT industries. Recourses of cloud computing are present in someone else's network i.e.; cloud service provider's network and the resources are accessed remotely by the cloud user via public channel. Due to the characterof cloud computing and openness of public channel the data in the cloud is vulnerable. Attackers can easily manipulatethe data. To overcome that AKA protocol is used. It allows a cloud service provider and a user to establisha secure channel. The existing AKA protocol suffer from some challenges like realizing low connection delay,eliminating certificate management problem, enhancing user privacy and avoiding bad randomness. To overcomethis, we use certificateless 0-RTT protocol it speeds up the establishment of the secure channel. The protocol does not need for the certificates to bind the public keywith entity's identity which solves the certificate management problem. Concrete security analysis protocol is also used this gives strong security to user privacy and bad randomness resistance.

**KEYWORDS**: Cloud Computing, Key agreement, Secure communication 0-RTT.

## I. INTRODUCTION

**Cloud computing** is the on-demand delivery of IT resources via the internet with pay-as-you-go pricing. Instead of buying, owning and maintaining physical data centres and servers we can access technology services, such as computing power, storage and databases, on an as needed basis from a cloud provider. Organisations of every type, size and industry are using the cloud for a wide variety of use cases, such as data backup, disaster recovery, email, virtual desktops, software development and testing, big data analytics and customer facing web applications. For example, health care companies to develop more personalizes treatments for patients. With cloud computing business can become more agile, reduce cost, instantly scale, and deploy globally in minutes. Cloud computing gives you instant access to a broad range of technologies so we can innovate faster and build nearly anything we can imagine from infrastructure services such as compute, storage and databases, to IoT, machine learning data analytics and much more.

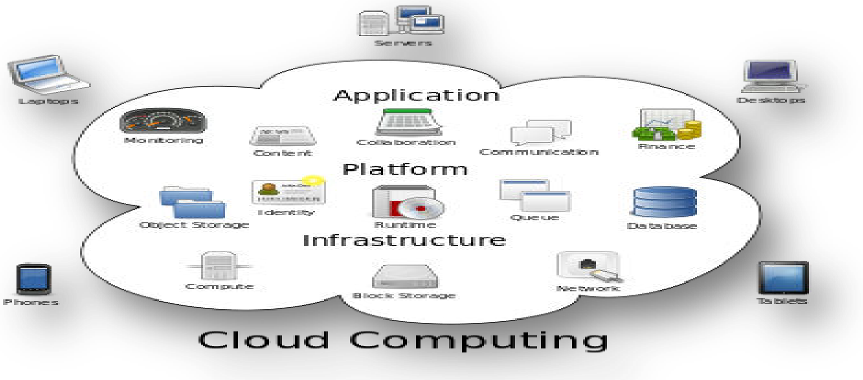


Figure 1: Structure of Cloud Computing

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

CLOUD computing has become as one of the fastest growing emerging technology of the IT industry in LOUD computing has become as one of the fastest recent years. It integrates a large number of virtual resources (e.g., computing power, storage, platforms, and services) and aims to maximize the effectiveness of the resources. Remote cloud users can access to those resources over the Internet using terminals, and get on-demand services by the model of pay-as-you-need. Successful examples include Amazons S3 and EC2, Microsoft Azure, Google App Engine and Rack space etc. This new computing model reduces start-up and operating costs and increases the agility of the users. Its benefits are being realized by more and more companies and individuals who are increasingly turning IT solutions to cloud computing. While enjoying the advantages of cloud computing, its unique architectural features also raise some security challenges which cannot be ignored In cloud computing, resources are usually in someone else's network, i.e., the network of a cloud service provider (CSP), and typically accessed remotely by the cloud users via public channels.

Processing is done remotely and the output is returned upon completion of required processing [2], [3]. Due to the characters of cloud computing and the openness of the public channels, an attacker can perform various attacks, such as impersonation, eavesdropping, forging and tampering. Therefore, authentication and confidentiality mechanisms have to be provided for the communications between a cloud user and CSP, so that only the authenticated users can access the resources and any attacker cannot violate the authentication and confidentiality of the messages exchanged. Authenticated key agreement (AKA) [4]–[6] is a widely used tool to achieve above goals, which allows a CSP and a user to establish a secure channel by agreed on a shared session key. Besides, user privacy is also of great concern in cloud computing, which prevents an attacker from identifying whether two messages are from the same cloud user. The data in cloud may contain sensitive information, e.g., medical records, financial data. If user privacy is not considered, anattacker may eavesdrop the communications to a cloud. Based on which, the attacker may deduce sensitive information, including who are using the cloud, how often, and what amount of data is being exchanged [7], [8], even the communications are encrypted. More seriously, if an attacker finds public figures (e.g., enterprise executives, famous stars) or other sensitive persons are the customs of the cloud, it may increase the attacker's possibility of corrupting the cloud. In fact, an attacker may launch some powerful attacks (e.g., targeted phishing attacks [9]) to steal cloud users' personal information (e.g., Celebrity iCloud Hack [10]). Or an attacker may launch a denial-of-service attack [11] to block the connections between a cloud used for diagnosis and a patient. Causing the disconnection at acritical time may bring terrible consequence and even lead to death. Therefore, user privacy is of particular concern in cloud computing and must be protected.

## II. RELATED WORK

In [1] authors define and solve the effective yet secure ranked keyword search over encrypted cloud data. We used order preserving symmetric encryption to protect the cloud data. Even though there are lots of searching techniques available, they are not giving efficient search results.

In [2] it presents protecting the contents of audit logs from unauthorized parties (ie, encrypting it), while making it efficiently searchable by authorized auditors poses a problem. We describe an approach for constructing searchable encrypted audit logs which can be combined with any number of existing approaches for creating tamper-resistant logs.

In [3] Attribute-based encryption (ABE) is a new vision for public key encryption that allows users to encrypt and decrypt messages based on user attributes. For example, a user can create a ciphertext that can be decrypted only by other users with attributes satisfying.

In [4] Here "public-key" refers to the fact that ciphertexts are created by various people using Alice's public key. Consider a mail server that stores various messages publicly encrypted for Alice by others. We define the concept of public key encryption with keyword search and give several constructions.

In [5] In a ciphertext-policy attribute-based encryption (CA-ABE) system, description keys are defined over attributes shared by multiple users. Given a decryption key, it may not be always possible to trace to the original key owner.

In [6] Attribute-based encryption (ABE) is a vision of public key encryption that allows users to encrypt and decrypt messages based on user attributes. This functionality comes at a cost. The decryption time is proportional to the number of attributes used during decryption.

In [7] Conjunctive keyword searchable encryption scheme makes it possible to retrieve several keywords in encrypted data at one time. In this paper, we present a conjunctive keyword searchable encryption with constant pairing, short cipher text and trapdoor in the standard model. We also propose two concrete constructions and give their security analysis.

## III. PROPOSED SYSTEM

In the proposed system cloud user's public key is just his identity and a public value chosen by himself while his private key is jointly generated by a trusted entity and himself. Since no certificate is needed, our protocol eliminates the certificate management problem for the potential abundant numbers of cloud users. With the private key, a cloud user may establish a secure channel with a previously visited CSP and send an encrypted message to the CSP simultaneously in 0-RTT which improves users' quality of experience (e.g., fast connection to a CSP, low connection failure rate). We note that for the first communication between a cloud user and a CSP, other heavier mutual authentication protocols have to be used, which is beyond the discussion of this paper. However, the heavy mutual authentication protocol only needs to be run once. Then the cloud user and the CSP may use our protocol to establish a secure channel. Simulations show that our protocol is more efficient than all the existing AKA protocols in CL-PKC (that support 0-RTT or user privacy). Further, even compared with the well-known DH protocol [20] (which is the most efficient one-RTT key agreement protocol), our protocol is about 2 times more efficient that the DH protocol in the real-world applications.

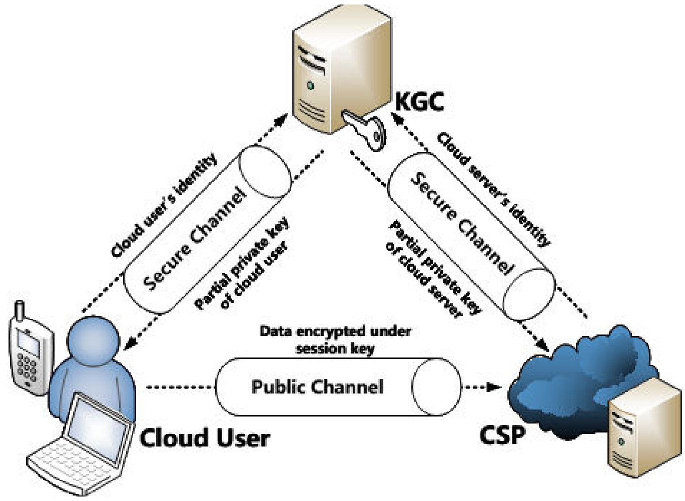


Figure 2: System Model

We propose our concrete anonymous authentication protocol for cloud computing in 4 stages.

1. System Setup: The KGC (key generation center) takes as input a security parameter κ, and generates the system parameters params and masterkey as follows:• Generate q, P, e, Gˆ 1, G2 as defined above. • Choose a random value s ∈ Z ∗ q as the master-key and compute P0 = sP. • Choose four cryptographic hash functions H1 : G1 → {0, 1} t , H2 : {0, 1} ∗ → G1, H3 : {0, 1} ∗ → Z ∗ q , H4 : {0, 1} ∗ → {0, 1} l . The KGC publishes the system parameters params = {q, G1, G2, e, P, P ˆ 0, H1, H2, H3, H4} and keeps the master key s secretly
2. Extract: The cloud service provider S/cloud user U with identity ids/idu generates his private-public key pair and/or seed with the help of KGC.
3. Registration and establishment: The main aim is to get certificateless 0-RTT anonymous AKA protocol. As a 0-RTT protocol, we require that a cloud user has already visited a CSP, and stored the identity and public key of the CSP locally (which are about 512 bits). However, this protocol only needs to be run once. This implies the cloud user has already authenticated the CSP. Let U's privatepublic key pair be (Su = (xu, Du),(idu, Pu)), U's seed be xk and S's private-public key pair be (Ss = (xs, Ds),(ids, Ps)).
4. Key- update: To update the seed of U, U just needs to run the seed generation algorithm in U-Private Public-Extract. In order to update the private key U, U has to run both U-Partial PrivateExtract and U-Private Public-Extract.

## IV. SYSTEM STUDY

### A) Feasibility Study

The Feasibility of project provides the various constraints to the quality of being weak or strong to plan the purpose of the business needs. To estimate the costs, performance, the designed implementation and the resource being defined for the environment. The various accepts that perform through the description of project, the operation of technical knowledge, managing the resources and mainly capable for the success. It is carried out during the proposed system; the future requirements may also include the level of system resources.

The feasibility study contains the three key:

- ○ Economic Feasibility
- ○ Technical Feasibility
- ○ Social Feasibility

**B) Economic Feasibility**

The Economic Feasibility provides the constraints that determine the quality and identifying the purpose of project. It provides the estimation for possible technical requirements; the investment offered by organizer to develop a system and the technologies is often used for the customer needs.

**C) Technical Feasibility**

The study of technical feasibility provides the aspects of technical knowledge to determine the system requirements and also designing the system resources. The modernized development of system is implemented for attracting the customers to define the project. The technicality provides a highly quality of service for the client's satisfactions.

**D) Social Feasibility**

The study of social feasibility defines how the outside environment will accepts the system requirements. It is designed in such a way that how confidently and convincingly reaches to the user, the level of accepting the project and the defined requirement of project. The goal is to satisfy the clients required outcome and also to manage how the system to be used by user for further purpose.

## V. SYSTEM DESIGN

System design is very important for the supernova of the software, which is called asdesign phase. The designphase should satisfy the functional and non-functionalrequirements for the This document gives the design of the overall project. Softwaredevelopment is the phase effectiveness for satisfying all the constraints and objectives of the project. It mainly concentrates on the modules that needed for system. The designphase depends mainly on the specification of feasibility survey.

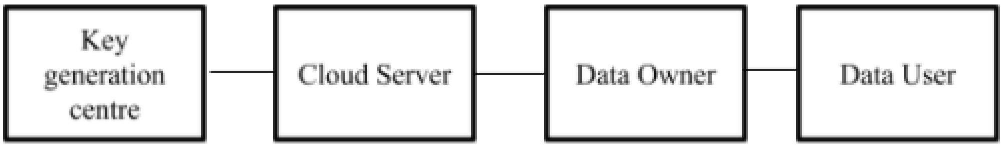


Figure 3: System design block diagram

**A) Data Flow Diagram:**

The information stream outline demonstrates the graphical portrayal, similar to game plans it is utilized to speak to the information through the sources of info, different sorts of information examination will be completed and the coveted yield will be produced. These parts will be utilized to demonstrate the framework and it will be displayed by to contemplate quickly regarding the information. In the framework outline the DFD will demonstrate the stream of whole parts. The stream of data will in arrangement of change utilizing this framework.

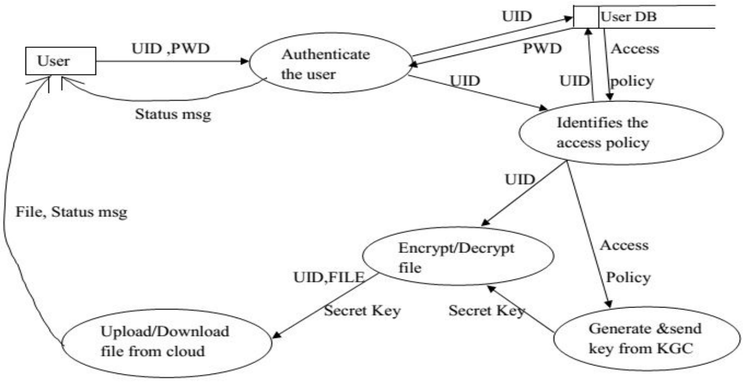


Figure 4: Data flow diagram

### B. Use Case Diagram:

An utilization case in programming designing and frameworks building is a portrayal of aframework'sconduct as it reacts to a demand that starts from outside of that framework. As itwere, an utilization case depicts "who" can do "what" with the framework being referred to.The utilization case method is utilized to catch a framework's behavioral necessities byspecifying situation driven strings through the useful prerequisites.

An utilization case in programming designing and frameworks building is a portrayal of a framework's conduct as it reacts to a demand that starts from outside of that framework. As it were, an utilization case depicts "who" can do "what" with the framework being referred to. The utilization case method is utilized to catch a framework's behavioral necessities by specifying situation driven strings through the useful prerequisites.

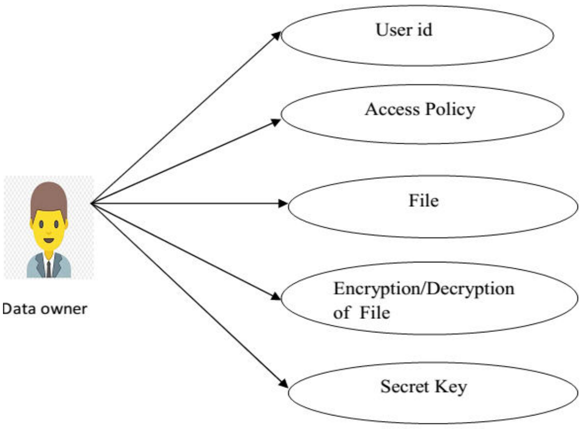


Figure 5: Use case for data owner

A use case diagram in the Unified Modelling Language (UML) is a type of behaviouraldiagram defined by and createdfrom a Use-case analysis. Its purpose is to present a graphicaloverview of the functionality provided by a system interms of actors, their goals(represented as use cases), and any dependencies between those use cases. The main purposeof a use case diagram is to show what system functions are performed for which actor. Rolesof the actors in the system can be depicted.

## VI. Conclusion

In order to allow a cloud server to search on encrypted data without learning the underlying plaintexts in the publickey setting, Boneh [7] proposed a cryptographic primitive called public-key encryption with keyword search (PEKS). Since then, considering different requirements in practice, e.g., communication overhead, searching criteria and security enhancement, various kinds of searchable encryption systems have been put forth. However, there exist only a few public-key searchable encryption systems that support expressive keyword search policies, and they are all built from the inefficient composite-order groups [17]. In this approach, we focused on the design and analysis of public-key searchable encryption systems in the prime-order groups that can be used to search multiple keywords in expressive searching formulas. Based on a large universe key-policy attribute-based encryption scheme given in [18], we presented an expressive searchable encryption system in the primeorder group which supports expressive access structures expressed in any monotonic Boolean formulas. Also, we proved its security in the standard model, and analysed its efficiency using computer simulations.

## References

[1] L. Zhang, X. Meng, K. Choo, Y. Zhang, and F. Dai, “Privacypreserving cloud establishment and data dissemination scheme for vehicular cloud,” IEEE Transactions on Dependable and Secure Computing, 2018, doi: 10.1109/TDSC.2018.2797190.

[2] M. Jouini and L. Rabai, “A security framework for secure cloud computing environments,” in Cloud Security: Concepts, Methodologies, Tools, and Applications, 2019, pp. 249–263.

[3] J. Li, L. Zhang, J. Liu, H. Qian, and Z. Dong, “Privacy-preserving public auditing protocol for low-performance end devices in cloud,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2572–2583, 2016.

[4] H. Krawczyk and H. Wee, “The OPTLS protocol and TLS 1.3,” in 2016 IEEE European Symposium on Security and Privacy, 2016, pp. 81–96.

[5] B. Hale, T. Jager, S. Lauer, and J. Schwenk, “Simple security definitions for and constructions of 0-rtt key exchange,” in 15th International Conference on Applied Cryptography and Network Security, 2017, pp. 20–38.

[6] L. Zhang, “Key management scheme for secure channel establishment in fog computing,” IEEE Transactions on Cloud Computing, doi: 10.1109/TCC.2019.2903254

[7] G. Han, X. Miao, H. Wang, M. Guizani, and W. Zhang, “CPSLP: a cloud-based scheme for protecting source location privacy in wireless sensor networks using multi-sinks,” IEEE Transactions on Vehicular Technology, vol. 68, no. 3, pp. 2739–2750, 2019.

[8] C. A. Ardagna, M. Conti, M. Leone, and J. Stefa, “An anonymous end-to-end communication protocol for mobile cloud environments,” IEEE Transactions on Services Computing, vol. 7, no. 3, pp.373–386, 2014.

[9] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, “Social phishing,” Communications of the ACM, vol. 50, no. 10, pp. 94–100, 2007.

[10] “Icloud Data Breach: Hacking and celebrity photos.” [Online]. Available: https://www.forbes.com/sites/davelewis/2014/ 09/02/icloud-data-breach-hacking-and-nude-celebrity-photos/ #4194819e2de7

[11] L. Garber, “Denial-of-service attacks rip the internet,” Computer, vol. 33, no. 4, pp. 12–17, 2000.

[12] Q. Pei, B. Kang, L. Zhang, K. Choo, Y. Zhang, and Y. Sun, “Secure and privacy-preserving 3D vehicle positioning schemes for vehicular ad hoc network,” EURASIP Journal on Wireless Communications and Networking, vol. 2018, no. 1, p. 271, 2018.

[13] E. Rescorla, “The transport layer security (TLS) protocol version 1.3,” no. RFC 8446, 2018. [Online]. Available: https: //www.rfc-editor.org/rfc/pdfrfc/rfc8446.txt.pdf

[14] “Introducing zero round trip time resumption(0-RTT).” [Online]. Available: https://blog.cloudflare.com/introducing-0-rtt/

[15] S. S. Al-Riyami and K. G. Paterson, “Certificateless public key cryptography,” in 9th International Conference on the Theory and Application of Cryptology and Information Security, 2003, pp. 452– 473.

[16] M. Alt, W. Barto, A. Fasano, and A. King, “Entropy poisoning from the hypervisor,” 2015. [Online]. Available: https://pdfs.semanticscholar.org/06cd/ 9aacf17a9c13fbb7e524a4e48e8edc756457.pdf

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ✆ 6381 907 438 ✉ ijircce@gmail.com

Scan to save the contact details

www.ijircce.com