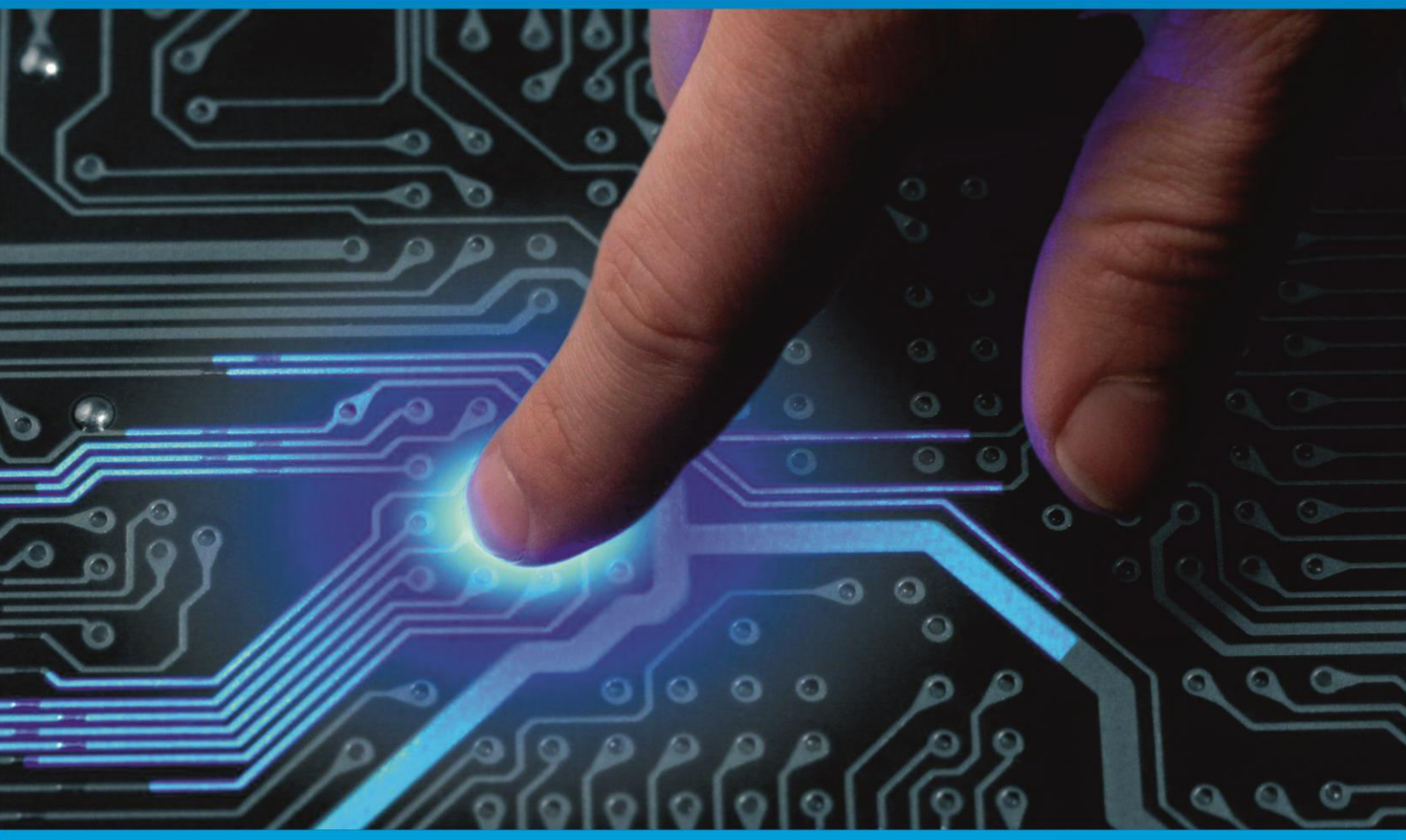
IJIRCCE

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



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905126 |

# Data Security Model for Mobile Cloud Computing

**Sachin Kothari[1], Dr. Ramesh B[2], Royce Christon Goveas[3], Sachin S[4], Yashvanth C S[5]**

UG Student, Dept. of CSE, Malnad College of Engineering, Hassan, India[1, 3, 4, 5]

Professor, Dept. of CSE, Malnad College of Engineering, Hassan, India[2]

**ABSTRACT:** Cloud Computing becomes the next generation architecture of IT Enterprise. In contrast to traditional solutions, Cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique feature, however, raises many new security challenges which have not been well understood. In cloud computing, both data and software are fully not contained on the user's computer; Data Security concerns arise because both user data and program are residing in Provider Premises. Clouds typically have single security architecture but have many customers with different demands. Every cloud provider solves this problem by encrypting the data by using encryption algorithms. But there are also chances that the cloud service is not trustworthy, to overcome this problem. This paper introduces a new model called V-CRT methodology which overcomes the basic problem of cloud computing data security. We present the data security model of cloud computing with a security vendor that eliminates the fear of misuse of data by the cloud service provider thereby improving data security.

## I. INTRODUCTION

Mobile Cloud Computing (MCC) is the combination of cloud computing and mobile computing to bring rich computational resources to mobile users, network operators, as well as cloud computing providers.The ultimate goal of MCC is to enable execution of rich mobile applications on a plethora of mobile devices, with a rich user experience. MCC provides business opportunities for mobile network operators as well as cloud providers.[5][6] More comprehensively, MCC can be defined as "a rich mobile computing technology that leverages unified elastic resources of varied clouds and network technologies toward unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere, anytime through the channel of Ethernet or Internet regardless of heterogeneous environments and platforms based on the pay-as-you-use principle.

Smartphones and tablets have become ubiquitous in our daily lives and quickly gained in usage and popularity, more consumers are relying on these devices, as their primary source of internet access. Smartphone devices are characterized by convenient

features, such as operating systems that can enable users not only to navigate, but also to interact with applications (e.g., playing games, chatting, recording videos and taking pictures). At the same time, continued and rapid increase of online applications and secure cloud services [1] results in an increase in demand for authentication. Authentication plays an important role [2] in how we interact with computers, mobile devices, the web, etc. For example, in recent years, more corporate information and applications have been accessible via the Internet and Intranet. Several employees are working from different distant spots and require entry to protected corporate files. In the meantime, it is possible for malicious/unauthorized users to get access to the system.

### *A. Cloud deployment model*

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand. The Cloud Computing model has three main deployment models. Based on the model, cloud computing is mainly classified into three major categories such as

- Public cloud
- Private cloud
- Hybrid cloud

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905126 |

1) Public Cloud - A public cloud is one in which the services and infrastructure are provided off-site over the internet. These clouds offer the greatest level of efficiency in shared resources. Public clouds are run by third parties, and applications from different customers are likely to be mixed together on the cloud's servers, storage systems, and networks.

2) Private Cloud - These clouds offer the greatest level of security and control, but they require the company to still purchase and maintain all the software and infrastructure, which reduces the cost savings.

3) Hybrid Cloud - Hybrid cloud is the combination of private cloud and public cloud. It includes combining the features of the public cloud and private cloud. This model increases the feasibility and scalability to a greater extent.

### *B. Service delivery models*

The three main cloud service delivery models are

• Infrastructure-as-a-Service (IaaS) - Infrastructure as a service are online services that provide high-level APIs used to dereference various low-level details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc.

• Platform-as-a-Service (PaaS) - Platform as a service is a category of cloud computing services that allows customers to provision, instantiate, run, and manage a modular bundle comprising a computing platform and one or more applications, without the complexity of building and maintaining the infrastructure typically associated with developing and launching the application(s); and to allow developers to create, develop, and package such software bundles.

• Software-as-a-Service (SaaS) - Software as a service (or SaaS) is a way of delivering applications over the Internet—as a service. Instead of installing and maintaining software, you simply access it via the Internet, freeing yourself from complex software and hardware management.

## II. LITERATURE REVIEW

### A.*A fully homomorphic encryption scheme*

We propose the first fully homomorphic encryption scheme, solving an old open problem. Such a scheme allows one to compute arbitrary functions over encrypted data without the decryption key—i.e., given encryptions E(m1), ..., E( mt) of m1, ..., m t, one can efficiently compute a compact ciphertext that encrypts f(m1, ..., m t) for any efficiently computable function f.

Fully homomorphic encryption has numerous applications. For example, it enables encrypted search engine queries—i.e., a search engine can give you a succinct encrypted answer to your (boolean) query without even knowing what your query was. It also enables searching on encrypted data; you can store your encrypted data on a remote server, and later have the server retrieve only files that (when decrypted) satisfy some boolean constraint, even though the server cannot decrypt the files on its own. More broadly, it improves the efficiency of secure multiparty computation.

In our solution, we begin by designing a somewhat homomorphic "bootstrappable" encryption scheme that works when the function f is the scheme's own decryption function. We then show how, through recursive self-embedding, bootstrappable encryption gives fully homomorphic encryption.

### B.*Hybrid encryption for cloud database security*

In the cloud computing environment the new data management model is in use nowadays that enables data integration and access on a large scale cloud computing as a service termed as Database-as-a-service (DAAS). Through which service provider offers customer management functionalities as well as the expensive hardware. Data privacy is the major security determinant in DAAS because data will be shared with a third party; an untrusted server is dangerous and unsafe for the user. This paper shows a concern on the security element in cloud environments. It suggests a technique to enhance the security of cloud databases. This technique provides flexible multilevel and hybrid security. It uses RSA, Triple DES and Random Number generator algorithms as an encrypting tool.

### C.*Lightweightand secure database encryption using tsfs algorithm*

Challenges for security in databases are increased due to the enormous popularity of e-business. In recent years, insider attacks gathered more attention than periodic outbreaks of malware. Database systems are usually deployed deep inside the company network and thus insiders have the easiest opportunity to attack and compromise

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905126 |

them, and then steal the data. So data must be protected from inside attackers also. Many conventional database security systems are proposed for providing security for databases, but still the sensitive data in databases are vulnerable to attack because the data are stored in the form of plaintext only. Database encryption is the only solution to avoid the risk posed by this threat. This paper focuses on a security solution for protecting data-at-rest, specifically protecting the sensitive data that resides in databases by using TSFS algorithm with three keys thus it provides more security for databases. This algorithm improves the efficiency for executing the queries in the database by encrypting only the sensitive data.

D.***Using in-memory encrypted databases on the cloud***

Storing data in the cloud poses a number of privacy issues. A way to handle them is supporting data replication and distribution on the cloud via a local, centrally synchronized storage. In this paper we propose to use an in-memory RDBMS with row-level data encryption for granting and revoking access rights to distributed data. This type of solution is rarely adopted in conventional RDBMSs because it requires several complex steps. In this paper we focus on implementation and benchmarking of a test system, which shows that our simple yet effective solution overcomes most of the problems.

E. ***A commutative encryption scheme based on ElGamal encryption***

A commutative encryption is a kind of an encryption system that enables a plaintext to be encrypted more than once using different users' public keys. In this system, decryption is not required before the encryption/re-encryption processes. Moreover, the resulting ciphertext can be decrypted by the designated decrypters without considering the order of public keys used in the encryption/re-encryption processes. In other words, the order of keys used in encryption and in decryption do not affect the computational result. Commutative encryption schemes are found useful in many real life applications such as in secret sharing, database integration and etc. However, regardless of its usefulness, few papers demonstrate how to construct such a kind of a commutative encryption. In this paper, we propose a new commutative encryption scheme based on the ElGamal encryption and provide the security proof in the random oracle model.

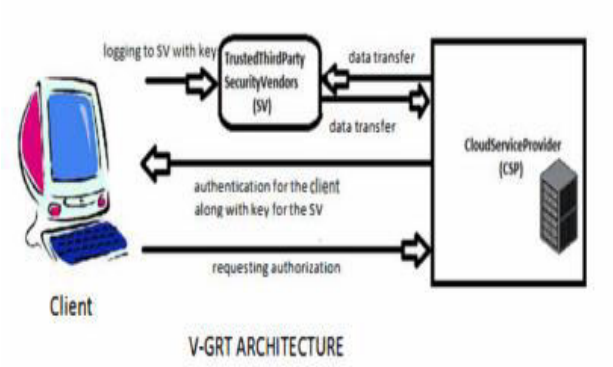
## III. MECHANISM OF PROPOSED SYSTEM

*A.**Problem Statement***

One of the main drawbacks of cloud is that there are too many possibilities for the cloud service provider for the misuse of the data that is stored in their data center by the client. Due to this, whatever methods that are proposed don't have a direct impact to reduce this problem. There will be issues continuing in the cloud computing until the cloud service provider knowledge about the data is prohibited. There is also repeated usage of OTP methods in the cloud computing techniques which makes this system an inefficient one.

*B.**Model Design: V-GRT architecture***

The proposed architecture is shown in the Fig.




V-GRT ARCHITECTURE

the operations are described in the following steps:

1) Username and the Password provided by the client to the cloud service provider. The password is encrypted by Hybrid Encryption method such as RSA, Caesar cipher and alphabetic encryption

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905126 |

2) Cloud Service Provider (CSP) authenticates the user by verifying username and password by decryption and sends with the login key for the Security Vendor.
3) User space in CSP and the memory address allocated for the user is given by the Cloud Service Provider to the Security Vendor.
4) Login key for Security vendor
5) User authenticated with key provided by Cloud Service Provider
6) User selects the encryption method for various options that CSP does not aware of and stores the data
7) Security vendor sends the encrypted data to Cloud Service Provider.

## IV. COMPARISON

### A. *Exsisting System:*

Huang and Tso proposed an asymmetric encryption mechanism for databases in the cloud. In the proposed mechanism, the commutative encryption is applied on data more than once and the order of public/private key used for encryption/decryption does not matter.
Re encryption mechanism is also used in the proposed scheme which shows that the cipher-text data is encrypted once again for duality.

**Disadvantages**

Data confidentiality occurs because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their sensitive data in cloud storage directly. Simple encryption is faced with the key management problem and cannot support complex requirements such as query, parallel modification, and fine grained authorization.

One of the main drawbacks of cloud is that there are too many possibilities for the cloud service provider for the misuse of the data that is stored in their data center by the client. Due to this, whatever methods that are proposed don't have a direct impact to reduce this problem. There will be issues continuing in the cloud computing until the cloud service provider knowledge about the data is prohibited. There is also repeated usage of OTP methods in the cloud computing techniques which makes this system an inefficient one.

### B. *Proposed system*

1) Username and the Password provided by the client to the cloud service provider. The password is encrypted by Hybrid Encryption method such as RSA, Caesar cipher and alphabetic encryption
2) Cloud Service Provider (CSP) authenticates the user by verifying username and password by decryption and sends with the login key for the Security Vendor.
3) User space in CSP and the memory address allocated for the user is given by the Cloud Service Provider to the Security Vendor.
4) Login key for Security vendor
5) User authenticated with key provided by Cloud Service Provider
6) User selects the encryption method for various options that CSP does not aware of and stores the data
7) Security vendor sends the encrypted data to Cloud Service Provider

**Advantages of proposed system**

- More Secure System
- Results show better performance evaluation when compared with existing system

## V. CONCLUSION

Data and privacy protection are the primary problems that need to be solved in cloud computing. Data Security and privacy issues exist in all levels of cloud service. The above mentioned model is fruitful in getting the user to trust the cloud computing so that the user is able to store confidential data over the cloud computing. The Encryption Algorithm applicability provides the flexibility in range and sequence to the user's choice because of the various Methods a user can apply all or omit any in any order. Even if the user does not select any encryption technique, then a random number algorithm will be implemented by default thus providing at least a single level of security. The opted sequence will also be stored in the database so that the decryption may be possible. The negative effect of this scheme is that it creates an overhead on the query performance due to multilevel encryption and decryption but for the sake of security the

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905126 |

performance issue can be overlooked as we are concerned with only a small amount of data like that of passwords and not the large files. In this way we can conclude that security vendors enhance security with the help of multilevel hybrid encryption.

## REFERENCES

[1]. C. Gentry, "A fully homomorphic encryption scheme [Ph.D. thesis]", International Journal of Distributed Sensor Networks, Stanford University, 2009.
[2]. D. Boneh, "The decision Diffie-Hellman problem", Algorithmic NumberTheory. 2008.
[3]. A. Kaur and M. Bhardwaj, "Hybrid encryption for cloud database security", Journal of Engineering Science Technology, 2010.
[4]. R. Arora, A. Parashar, and C. C. T. Transforming, "Secure user data in cloud computing using encryption algorithms", International Journal of Engineering Research and Applications, June 2013.
[5]. D. Manivannan and R. Sujarani, "Lightweight and secure database encryption using tsfs algorithm", Proceedings of the International Conference on Computing Communication and Networking Technologies ICCCNT '10.
[6]. F. Pagano and D. Pagano, "Using in-memory encrypted databases on the cloud", Proceedings of the 1 st IEEE International Workshop on Securing Services on the Cloud (TWSSC '11).
[7]. K.Huang and R. Tso, "A commutative encryption scheme based on ElGamal encryption", Proceedings of the 3rd International Conference on Information Security and Intelligent Control (ISIC '12), August 2012.
[8]. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy Preserving multi-keyword ranked search over encrypted cloud data", IEEE Transactions on Parallel and Distributed Systems, 2012.
[9]. M. A. AlZain, B. Soh, and E. Pardede, "Mcdb: using multi clouds to ensure security in cloud computing", Proceedings of the IEEE 9th International Conference on Dependable, Autonomic and Secure Computing (DASC '11).
[10]. C. P. Ram and G. Sreenivaasan, "Security as a service (sass): securing user data by coprocessor and distributing the data". Proceedings of the 2nd International Conference on Trends in Information Sciences and Computing, (TISC '10).
[11]. M. AsadArfeen, K. Pawlikowski, and A. Willig, "A framework for resource allocation strategies in cloud computing environment", Proceedings of the 14th Annual IEEE International Computer Software and Applications Conference Workshops (COMPSAC WII).
[12]. P. Victer Paul, D. Rajaguru, N. Saravanan, R. Baskaran and P. Dhavachelvan, "Efficient service cache management in mobile P2P networks", Future Generation Computer Systems, Elsevier, Volume 29, Issue 6, August 2013, Pages 1505-1521.
[13]. E. M.Mohamed, H. S. Abdelkader, and S. El-Etriby, "Enhanced data security model for cloud computing" , Proceedings of the 8th International Conference on Informatics and Systems (INFOS '12).
[14]. S. Biedermann and S. Katzenbeisser, "POSTER: event-based isolation of critical data in the cloud", Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2012.
[15]. C. Delettre, K. Boudaoud, and M. Riveill, "Cloud computing, security and data concealment", Proceedings of the 16th IEEE Symposium on Computers and Communications (lSCC '11).
[16]. Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "Fade: secure overlay cloud storage with file assured deletion", Security and Privacy in Communication Networks, 2011.
[17]. P. Victer Paul, N. Saravanan, S.K.V. Jayakumar, P. Dhavachelvan and R. Baskaran, "QoS enhancements for global replication management in peer to peer networks", Future Generation Computer Systems, Elsevier, Volume 28, Issue 3, March 2012, Pages 573-582.
[18]. A. Rao, "Centralized database security in cloud", International Journal of Advanced Research in Computer and Communication Engineering, 2011
[19]. P. Victer Paul, T. Vengattaraman, P. Dhavachelvan, "Improving efficiency of Peer Network Applications by formulating Distributed Spanning Tree", Third International Conference on Emerging Trends in Engineering & Technology (lCETET-201O), IEEE, India, May 2010. pp. 813-818.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details