ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.6

# Additional Protection in Public Cloud using Random Key Genereation

P.karthikeyan[1], Rejees Jenifa[2], V.Nivedha[3]
Assistant Professor[1, 2], MCA Student[3]
Department of Computer Science and Engineering
Veltech High-Tech Dr.Rangarajan Dr.Sakunthla Engineering College, Chennai, India

**Abstract:**
Remote information get to control is of urgent significance in broad daylight cloud. In light of its own slants, the information proprietor predefines the entrance arrangement. At the point when the client fulfills the information proprietor's entrance approach, it has the privilege to get to the information proprietor's remote information. Keeping in mind the end goal to enhance adaptability and effectiveness of remote information get to control, trait based encryption (for short, ABE) is utilized to understand the remote information fine-grained get to control. For the low-limit terminals, undeniable outsourced unscrambling is an extremely alluring procedure. In the genuine application situations, the client's characteristics are normally overseen by numerous experts. At the point when some approved clients get to some delicate remote information, they would like to protect their character security. From the two focuses, we propose a mysterious appropriated fine-grained get to control convention with unquestionable outsourced unscrambling out in the open cloud. VOD-ADAC is a novel idea which is proposed without precedent for the paper. By embracing the pen name, the client's high obscurity can be accomplished by much of the time changing the autonomous aliases some very social spots. This paper formalizes the framework model and security model of VOD-ADAC convention. At that point, by utilizing cross breed encryption system of dispersed ABE and symmetric encryption, a solid VOD-ADAC convention is outlined from the bilinear pairings. Through security examination and execution investigation, our proposed VOD-ADAC convention is provably secure and effective.

## I. INTRODUCTION:

Along with the development of cloud computing, increasingly agencies and individuals upload their statistics to public cloud server (for quick, PCS). They will delegate PCS to save and control their far off information. By the usage of public cloud, the companies and people are relieved of the load of storage management, general statistics get right of entry to with impartial geographical locations, capital expenditure on hardware, and so forth. Public cloud can provide statistics garage carrier, computation service, and many others. Thus, cloud computing attracts all sorts of customers. For the low-ability terminals, outsourced computing makes them successfully get right of entry to the remote facts. Since PCS takes element within the decryption process, the cheating PCS need to be defended. Verifiable outsourced decryption may be used to shield the cheating PCS. At the equal time, so one can successfully guard the far off statistics confidentiality, the uploaded records might be encrypted by way of combining the allotted ABE encryption and symmetric encryption. For the real scenario, the customers' attributes are controlled by many one of a kind government. Thus, the allotted (i.E., multiauthority) ABE with verifiable outsourced computing can be used for the allotted first-class-grained access manipulate in public cloud. When the customers get entry to the faraway touchy facts, they opt to preserve their identification privateness. Thus, based at the dispensed ABE with verifiable outsourced computing, and the opposite novel cryptographic components, we can study VODADAC protocol for the first time.

**OBJECTIVE:**
In the actual surroundings, the consumer's attributes are managed with the aid of exclusive government, e.g, nationality, academic title, career, and so forth. Thus, every user has many characteristic secret keys which come from distinct authorities. When the user uses the low-ability terminals, e.g, cellular phone, etc, the person has to apply the outsourced computation. When PCS takes part inside the outsourced computation, the cheating PCS might also ship wrong reaction to the person on the way to save its personal computation overhead.

**SCOPE OF THE PROJECT:**
In the actual surroundings, the consumer's attributes are managed with the aid of exclusive government, e.g, nationality, academic title, career, and so forth. Thus, every user has many characteristic secret keys which come from distinct authorities. When the user uses the low-ability terminals, e.g, cellular phone, etc, the person has to apply the outsourced computation. When PCS takes part inside the outsourced computation, the cheating PCS might also ship wrong reaction to the person on the way to save its personal computation overhead.

## II. LITERATURE SURVEY:

The anonymous ABE provides an interesting security feature receiver anonymity in addition to data confidentiality and fine-grained access control of ABE. While storing encrypted documents in public cloud, an efficient search functionality facilitates user to retrieve a subset of documents for which the user has access rights on stored documents. We proposed an anonymous attribute based search- able encryption scheme which facilitates user to retrieve only a subset of documents pertaining to his chosen keyword. User can upload documents in public cloud in an encrypted form, search documents based on keyword and retrieve documents without revealing his identity.

The scheme is proven se- cure under the standard adversarial model. The scheme is efficient, as it requires small storage for user's decryption key and reduced computation for decryption in comparison to other schemes[1]. The Personal Health Records are maintained in a data server under the cloud environment. A novel framework of secure sharing of personal health records has been proposed in this paper. Public and Personal access models are designed with security and privacy enabled mechanism. The framework addresses the unique challenges brought by multiple PHR owners and users, in that the complexity of key management is greatly reduced. The attribute-based encryption model is enhanced to support operations with MAABE[2].the Cloud computing is a revolutionary computing paradigm which enables flexible, on-demand and low-cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns emerge from it. Various schemes based on the Attribute-Based Encryption have been proposed to secure the cloud storage. However, most work focuses on the data contents privacy and the access control, while less attention is paid to the privilege control and the identity privacy. In this paper, we present a semi-anonymous privilege control scheme AnonyControl to address not only the data privacy but also the user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semi-anonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, we present the AnonyControl- F which fully prevents the identity leakage and achieve the full anonymity. Our security analysis shows that both AnonyControl and AnonyControl-F are secure under the DBDH assumption, and our performance evaluation exhibits the feasibility of our schemes[3].we present two fully secure functional encryption schemes. Our first result is a fully secure attribute-based encryption (ABE) scheme. Previous constructions of ABE were only proven to be selectively secure. We achieve full security by adapting the dual system encryption methodology recently introduced by Waters and previously leveraged to obtain fully secure IBE and HIBE systems. The primary challenge in applying dual system encryption to ABE is the richer structure of keys and ciphertexts. In an IBE or HIBE system, keys and ciphertexts are both associated with the same type of simple object: identities. In an ABE system, keys and ciphertexts are associated with more complex objects: attributes and access formulas. We use a novel information-theoretic argument to adapt the dual system encryption methodology to the more complicated structure of ABE systems. We construct our system in composite order bilinear groups, where the order is a product of three primes. We prove the security of our system from three static assumptions. Our ABE scheme supports arbitrary monotone access formulas. Our second result is a fully secure (attribute-hiding) predicate encryption (PE) scheme for inner-product predicates. As for ABE, previous constructions of such schemes were only proven to be selectively secure. Security is proven under a non-interactive assumption whose size does not depend on the number of queries. The scheme is comparably ecient to existing selectively secure schemes. We also present a fully secure hierarchical PE scheme under the same assumption. The key technique used to obtain these results is an elaborate combination of the dual system encryption methodology (adapted to the structure of inner product PE systems) and a new approach on bilinear pairings using the notion of dual pairing vector spaces (DPVS) proposed by Okamoto and Takashima[4].As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for ¯ne-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE)[5].

## III. IMPLEMENTATION

In this we implement the coding part using eclipse. Below are the coding's that are used to generate the domain module for Cloud Computing. Here the proposed techniques are used in the coding part to Cloud to Cloud Interaction.we investigate the multi-keyword top-k search problem for big data encryption against privacy breaches, and attempt to identify an efficient and secure solution to this problem. Specifically, for the privacy concern of query data, we construct a special tree-based index structure and design a random traversal algorithm, which makes even the same query to produce different visiting paths on the index, and can also maintain the accuracy of queries unchanged under stronger privacy.

## IV. METHODOLOGY

**Java** is a programming language originally developed by James Gosling at Microsystems and released in 1995 as a core component of Sun Microsystems' Java platform. The language derives much of its syntax from C and C++ but has a simpler object model and fewer low-level facilities. Java applications are typically compiled to byte code that can run on any Java Virtual Machine (JVM) regardless of computer architecture. Java is general-purpose, concurrent, class-based, and object-oriented, and is specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere". Java is considered by many as one of the most influential programming languages of the 20th century, and is widely used from application software to web applications The java framework is a new platform independent that simplifies application development internet. Java technology's versatility, efficiency, platform portability, and security make it the ideal technology for network computing. From laptops to datacenters, game consoles to scientific supercomputers, cell phones to the Internet, Java is everywhere! .Java has been tested, refined, extended, and proven by a dedicated community. And numbering more than 6.5 million developers, it's the largest and most active on the planet. With its versatility, efficiency, and portability, Java has become invaluable to developers by enabling them to:

- Write software on one platform and run it on virtually any other platform

- Create programs to run within a Web browser and Web services
- Develop server-side applications for online forums, stores, polls, HTML forms processing, and more
- Combine applications or services using the Java language to create highly customized applications or services
- Write powerful and efficient applications for mobile phones, remote processors, low-cost consumer products, and practically any other device with a digital heartbeat

**Object Oriented**

To be an Object Oriented language, any language must follow at least the four characteristics.

- 1.Inheritance:It is the process of creating the new classes and using the behavior of the existing classes by extending them just to reuse the existing code and adding addition a features as needed.
- 2.Encapsulation: It is the mechanism of combining the information and providing the abstraction.
- 3.Polymorphism: As the name suggest one name multiple form, Polymorphism is the way of providing the different functionality by the functions having the same name based on the signatures of the methods.
- 4.Dynamic binding : Sometimes we don't have the knowledge of objects about their specific types while writing our code. It is the way of providing the maximum functionality to a program about the specific type at runtime.

**Java Server Pages**

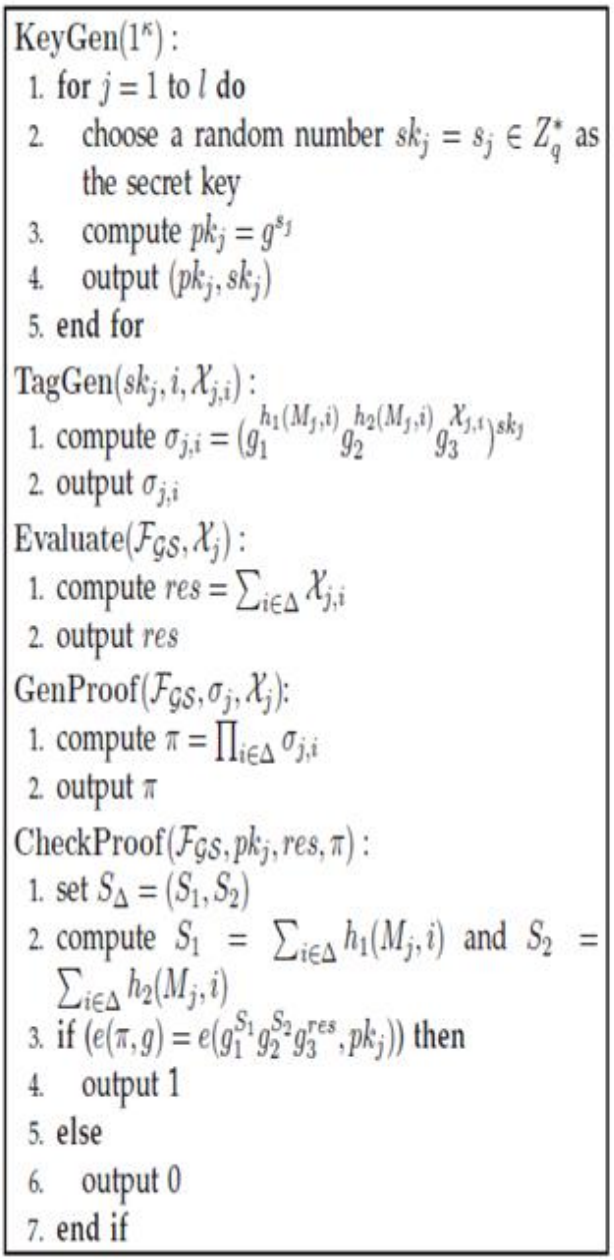
Java Server Pages or JSP for short is Sun's solution for developing dynamic web sites. JSP provide excellent server side scripting support for creating database driven web applications. JSP enable the developers to directly insert java code into jsp file, this makes the development process very simple and its maintenance also becomes very easy.

- JSP pages are efficient, it loads into the web servers memory on receiving the request very first time and the subsequent calls are served within a very short period of time.
- In today's environment most web sites servers dynamic pages based on user request. Database is very convenient way to store the data of users and other things. JDBC provide excellent database connectivity in heterogeneous database environment. Using JSP and JDBC its very cceasy to develop database driven web application.
- Java is known for its characteristic of "write once, run anywhere." JSP pages are platfJavaServer Pages
- JavaServer Pages (JSP) technology is the Java platform technology for delivering dynamic content to web clients in a portable, secure and well-defined way. The JavaServer Pages specification extends the Java Servlet API to provide web application developers with a robust framework for creating dynamic web content on the server using HTML, and XML templates, and Java code, which is secure, fast, and independent of server platforms.
- JSP has been built on top of the Servlet API and utilizes Servlet semantics. JSP has become the preferred request handler and response mechanism. Although JSP technology is going to be a powerful successor to basic Servlets, they have an evolutionary relationship and can be used in a cooperative and complementary manner.

Servlets are powerful and sometimes they are a bit cumbersome when it comes to generating complex HTML. Most servlets contain a little code that handles application logic and a lot more code that handles output formatting. This can make it difficult to separate and reuse portions of the code when a different output format is needed. For these reasons, web application developers turn towards JSP as their preferred servlet environment.

**Servlets**

- Earlier in client- server computing, each application had its own client program and it worked as a user interface and need to be installed on each user's personal computer. Most web applications use HTML/XHTML that are mostly supported by all the browsers and web pages are displayed to the client as static documents.
- A web page can merely displays static content and it also lets the user




navigate through the content, but a web application provides a more interactive experience. Any computer running Servlets or JSP needs to have a container. A container is nothing but a piece of software responsible for loading, executing and unloading the Servlets and JSP. While servlets can be used to extend the functionality of any Java- enabled server.

- They are mostly used to extend web servers, and are efficient replacement for CGI scripts. CGI was one of the earliest and most prominent server side dynamic content solutions, so before going forward it is very important to know the difference between CGI and the Servlets.

**Java Servlets**

Java Servlet is a generic server extension that means a java class can be loaded dynamically to expand the functionality of a server. Servlets are used with web servers and run inside a Java Virtual Machine (JVM) on the server so these are safe and portable. Unlike applets they do not require support for java in the web browser. Unlike CGI, servlets don't use multiple processes to handle separate request. Servets can be handled by separate threads within the same process. Servlets are also portable and platform independent.

## V. CONCLUSION:

Remote data access control is of crucial importance in public cloud. When the user satisfies the data owner's access policy, it has the right to access the data owner's remote data. In order to improve flexibility and efficiency of remote data access control. For the low-capacity terminals, verifiable outsourced decryption is a very attractive technique.. When some authorized users access some sensitive remote data, they hope to preserve their identity privacy. By adopting the pseudonym technique, the user's high anonymity can be achieved by frequently changing the independent pseudonyms at some highly social spots. This paper formalizes the system model and security model of VOD-ADAC protocol. Then, by using hybrid encryption technique of distributed ABE and symmetric encryption, a concrete VOD-ADAC protocol is designed from the bilinear pairings. Through security analysis and performance analysis, our proposed VOD-ADAC protocol is provably secure and efficient.

## FUTURE ENHANCEMENT

In the future research, we will study the dynamic policy and user revocation. In the real application, it is usual that the data owner adjusts its access policy according to the practical requirements. On the other hand, it is also usual that some users may be revoked. Thus, it is also necessary to add the security property of user revocation**.**

## VI. REFERENCE:


[1]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," Proc. EUROCRYPT, 2005, pp. 457-473.

[2]. V.Goyal, O. Pandey,A. Sahai, and B.Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proc. ACM Conf. Computer and Communications Security, 2006, pp. 89-98.

[3]. A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," Proc. EUROCRYPT, 2010, pp. 62-91.

[4]. B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," Proc. Public Key Cryptography, 2011, pp. 53-70.

[5]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," Proc. IEEE Symp. Security and Privacy, 2007, pp. 321-334.

[6]. J. Li, Y. Shi, Y. Zhang, "Searchable ciphertext-policy attributebased encryption with revocation in clou

[7]. X. Chen, J. Li, X. Huang, J. Li, Y. Xiang and D. S.Wong, "Secure outsourced attribute-based signatures", IEEE Transactions on Parallel and Distributed Systems, 25(12), 2014, pp. 3285-3294.

[8]. M. Chase, "Multi-authority attribute based encryption", Theory of Cryptography, 2007, pp. 515-534.

[9]. H. Qian, J. Li, Y. Zhang, J. Han,"Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation", International Journal of Information Security, 14(6), 2015, pp. 487-497.

[10]. S. M¨uller, S. Katzenbeisser, and C. Eckert, "Distributed attribute-based encryption", ICISC 2008, pp. 20-36.