© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 10 , Issue : 02 | April - June 2023

# EFFECTIVE SECURE SEARCH AND INTENSIVE QUERY RESULT VERIFICATION

**Chithra K[1], Gokulpriya D[2], Mounica S[3], Santhiya G[4], Nisha M[5]**

**Abstract**

More and more individuals are starting to save their data on the cloud as cloud computing becomes more commonplace. Easy accessibility, lower costs, rapid deployment, and adaptable resource management are just a few of the many advantages of cloud computing. The cloud enables businesses of all sizes to work together more creatively. While there are many advantages to using cloud computing, some people and businesses are wary of it due to privacy issues. Users are hesitant to save private information on the cloud, such as photographs, medical records, and trade secrets. Because losing control of sensitive data is a real possibility once it has been uploaded to the cloud.

**Keywords** – AES, data owner, admin, naive bayes.

## INTRODUCTION

In cloud computing, data owners may outsource their information to several consumers, each of whom may only be interested in a subset of the data. Keyword-based retrieval is a common method used for this purpose. We present a new searchable encryption system that takes use of recent developments in the field of cryptography, such as the Advanced Encryption Standard (AES). The suggested method involves the data owner encrypting the index that may be searched using Naive Bayes Classifier. With the rise of cloud computing, more and more private data is being stored there. Effective data usage is made difficult by the need of encrypting sensitive data before outsourcing. Owners of data on the cloud may allow several users to access it, but those users may only be interested in certain subsets of the data are curious about such details. Keyword-based retrieval is a common method used for this purpose. New innovations in the field of cryptography, such as encryption, have inspired us to suggest a new searchable encryption technique. This plan assumes. Naive Bayes, an indexing algorithm, is encrypted by the data owner and made searchable.

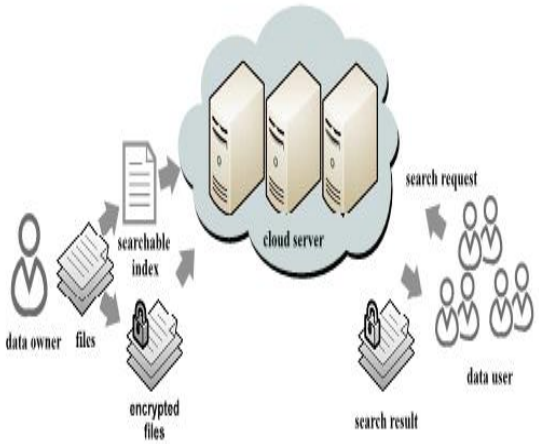


Fig 1 process of data retrieving

Secure keyword search over encrypted data has been the focus of numerous recent initiatives to improve data recovery from encrypted data. Reduced computational and communication overhead with qualified

© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 10 , Issue : 02 | April - June 2023

results. Therefore, a reliable secure query system should provide a means for the data user to validate query results. Each encrypted response from a query can be validated by our system, and we can also precisely determine how many and which qualifying data files the dishonest cloud server returns. The emphasis of the study shifts to how to search across encrypted cloud data quickly and safely. The AES algorithm is a block cypher because it uses a series of substitutions, permutations, and linear transformations executed on 16-byte data blocks. The majority of text categorization applications use naive bayes classifiers.

Using secure search methods over encrypted cloud data, a legitimate user may discreetly request information from the cloud server about specific data files of interest by sending encrypted query terms to the server.

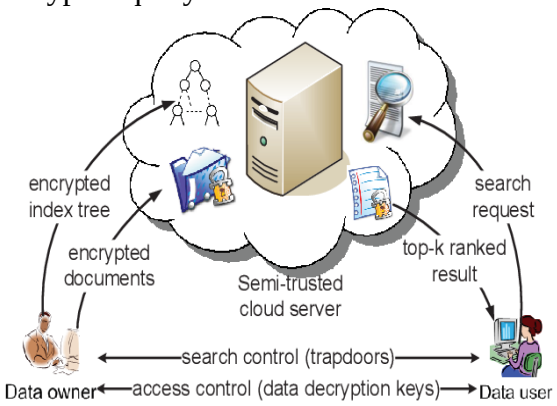


Fig.2. Outline of data retrieval based on keyword

## CLOUD COMPUTING ARCHITECTURE

On-demand self-service, ubiquitous network access, location-independent resource pooling, quick resource flexibility, usage-based pricing, and risk transference are just a few of the many reasons why cloud computing has been heralded as the next generation of IT design for organisations. Cloud computing is a game-changing innovation that is changing the way organisations utilise IT in fundamental ways. The centralization or outsourcing of data to the cloud is an essential part of this paradigm shift. From the point of view of users, both people and IT businesses, saving data remotely to the cloud in a flexible on-demand way is an attractive feature.

## WORKFLOW OF THE SYSTEM

Keyword indexes are encrypted and subject to careful query verification to provide a safe search experience. There are three steps to this.

1) Admin Login
2) Data Owner
3) Users At the outset, the Data Owner must provide their information. Once registered, data owners may use their login credentials to upload encrypted files to cloud storage and hashing algorithms. The Data Owner has the option of accepting or declining the data user's file request. Data Users must first register their information, and then verify their login using a secret key. Users of the data may make the request directly to the data providers.

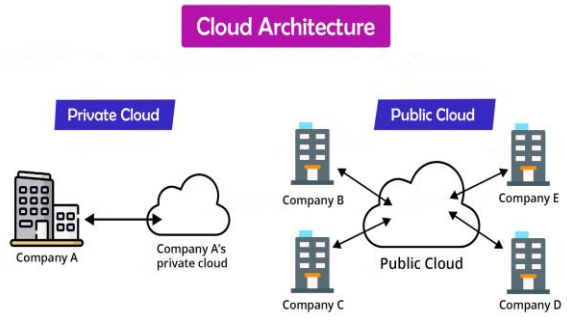


Fig.3.Cloud Computing

© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 10 , Issue : 02 | April - June 2023

**User self-provisioning**: In the cloud computing model, customers make purchases from the service provider directly, generally using a web form or dashboard. The client just forks over cash with each individual purchase.

**Advance provisioning**: Predetermined quantities of resources are contracted with customers in advance and prepared before service is rendered. A one-time or recurring payment is made by the consumer.

**Dynamic provisioning**: When a client requests a certain amount of resources, the supplier makes them available and removes them when they are no longer required. The client just pays for what they utilise.

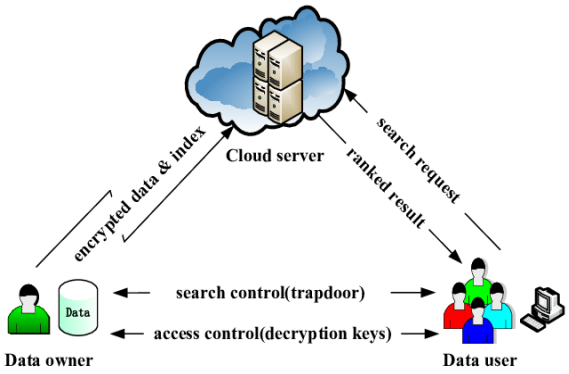


Fig 4 flow of data retrieve

**Stage1:DataOwner**

The first step in using the Data Owner module is for the Data Owner to register their information. Once registered, data owners may use their login credentials to upload encrypted files to cloud storage. The files you post to the cloud may be seen by him or her. The Data Owner has the option of granting the user's file request or denying it.

**Stage2:Admin**

When a user requests access to sensitive files, administrators approve their request. After registering, users must await admin permission before gaining access to the relevant documents for their specific inquiry. After reviewing the request's specifics, the administrator will grant the user access. A username and password are required to access the admin panel.

**Stage3:User**

Users must first register their information in the Data User module, and then verify their login with a secret key. All of the data owners' submitted files are searchable by Data Users. A request may be made to the files, and the owners of the data will be notified.

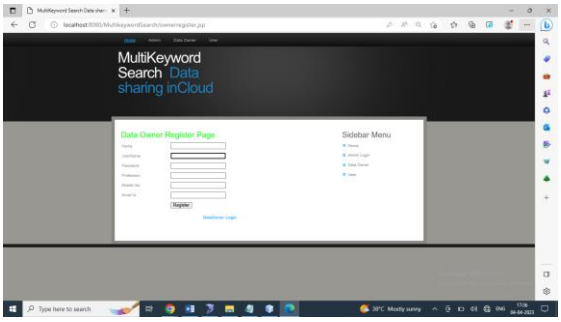


Fig.5. Registration Form

As we've seen, the major motivation for cloud computing is to enable safe and reliable data exchange. Client authentication allows access to the client's own data. Additionally, Two-Factor Authentication was implemented through a password-protected tunnel. This occurs often between e-Savings accounts. Clients need to be equipped with a device that displays a One-Time Password (OTP) in addition to a login and password (OTP). When two parties share information and neither can identify the other, we say that the data is anonymous. The high transmission and storage costs of big data make it

© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 10 , Issue : 02 | April - June 2023

unfeasible to aggregate data at a central location or at any of the individual locations. Anonymizing data implies concealing personal details and other sensitive information of an Personal privacy is maintained while certain data is made available to data consumers for analysis and mining purposes. An effective integrity auditing solution allows for validation, fault detection probabilities, modification by many users, and removal of infringing users. To protect the privacy of the users, the data should not be accessible unless both users provide their consent.

## SOFTWARES USED IN THE SYSTEM

### A.ECDA ALGORITHM

Research into Elliptic Curves (EC) is a vital part of the development of current asymmetric-key/public-key cryptography. Elliptic curve algebraic structure is the basis for this cryptography over finite fields. In order to provide the same degree of security as non-EC cryptography, Elliptic Curve Cryptography often employs lower key sizes. The Elliptic Curve Digital Signature Algorithm (ECDSA) is a keyed cryptographic algorithm that is a subset of the more widely used Digital Signature Algorithm (DSA).

### B. Java (programming language)

Source code for a Java software begins life as simple text files with a java extension. After that, the javac compiler turns those source files into executable class files. Instead of machine-specific instructions, a class file stores bytecodes, the language understood by the Java Virtual Machine (Java VM). Your programme is executed in a Java Virtual Machine instance via the java launcher tool. Java class files may be executed on Windows, Solaris TM Operating System (Solaris OS), Linux, and Mac OS thanks to the portability of the Java Virtual Machine (VM). Some virtual machines, like the Java HotSpot virtual machine, take extra actions during runtime to improve the speed of your programme. Finding speed bottlenecks and recompiling (to native code) commonly used areas of code are two examples of the many jobs that fall under this category. The Java Virtual Machine allows the same programme to function on many computers.

#### 1) The Java Platform

A platform is the hardware or software setting in which a computer application operates. Operating systems and hardware components often work together to build what we call a platform. Java is not a hardware-based platform in and of itself; rather, it is a software layer that operates atop other systems.

**Uses of Java:**

Blue is a smart card that makes use of the protected, portable, and object-oriented Java Card API and technology. Blue has a genuine on-board processing chip, enabling upgradeable and varied capabilities all on a single card. Any card from a third-party manufacturer that supports the Java Card Application Environment and has an Applet that complies with the Java Card API standard will execute the Applet (JCAE). Additional applets and features may be added to a customer's card after it has been issued, and existing applets can operate on the card.

· It's possible to use Java to chemistry.

© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 10 , Issue : 02 | April - June 2023

· In NASA also Java is used.
· In 2D and 3D applications java is used.
· In Graphics Programming also Java is used.
· In Animations Java is used.
· In Online and Web Applications Java is used.

**B. The Advantages of JSP**

Websites that Use CGI (ASP). Microsoft's ASP is a comparable platform. There are two main benefits of using JSP. To begin, the dynamic portion is written in Java rather than Visual Basic or any other Microsoft-specific language, making it more robust and user-friendly. Second, it works on non-Microsoft platforms and Web servers.

Absolute Servlets There is nothing you can accomplish with a servlet that you can't do with a JSP. Regular HTML is easier to write (and change!) than a million println commands that produce the HTML. Separating design and functionality allows you to delegate duties to the most qualified individuals. For example, your Web page designers can create the HTML, while your servlet developers can fill in the blanks with dynamic data.

Web Server Include Files (SSI).

SSI is a popular method of incorporating dynamic content into otherwise static Web pages. JSP is superior because it allows the usage of servlets.a distinct piece of software to create the variable element. Also, SSI isn't meant for real applications that utilise form data, link to databases, etc.; it's only for basic inclusions.

JavaScript. Client-side JavaScript based HTML generation is possible. This is a helpful feature, but it can only deal with circumstances in which the client's environment is the source of the dynamic information. JavaScript cannot access data sent over HTTP or a form, with the exception of cookies. In addition, JavaScript is client-side only, so it can't use server-side resources like databases, catalogues, and price information.

Plain old HTML Naturally, dynamic data cannot be included in standard HTML. Due to JSP's simplicity and efficiency, it is possible to enhance HTML pages with the addition of minimal quantities of dynamic data. Dynamic data was previously only used in the most advantageous situations due to its high price tag.

**OVERVIEW OF THE SYSTEM**

Authenticity of the goods by allowing the buyer to see its production and distribution records. Customers are able to monitor the full lifecycle of a product, from production to consumption, with the help of blockchain technology. There are three main players in this Blockchain-based anti-counterfeiting system for products: the manufacturer, the retailer, and the end user.

**Manufacturer:**

The serial number for the Product is created once the manufacturer login into their account and uploads the necessary information about the Product. If both the manufacturer's account and the wallet address are in our local database, the block will be added to the chain only if the manufacturer signs in with his own account and wallet.

**Supplier:**

© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 10 , Issue : 02 | April - June 2023

The supplier checks the product's serial number using the supplier account. Information about the items submitted by the manufacturer is available to the retailer. It then updates the Blockchain with additional information on the product, such as the store where it was purchased. The purchaser is free to read such information.

**Customer:**

Customers may verify the product's authenticity by looking up its unique serial number and seeing its transaction history. If the last location recorded for a product's serial number does not match the area where the goods was purchased, the buyer will be alerted that the product is counterfeit. The consumer learns that their serial number was likely duplicated.

## IMPLEMENTATION

The proposed system is known as the Fake Thing Identification System, and it will help consumers determine whether or not the product they are about to buy is authentic. The system was built using Java Server Pages, Java Script, Cascading Style Sheets, Structured Query Language, and Extensible Markup Language (XML).

Research into Elliptic Curves (EC) is a vital part of the development of current asymmetric-key/public-key cryptography. Elliptic curve algebraic structure is the basis for this cryptography over finite fields. In order to provide the same degree of security as non-EC cryptography, Elliptic Curve Cryptography often employs lower key sizes. The Elliptic Curve Digital Signature Algorithm (ECDSA) is a keyed-based variation of the Digital Signature Algorithm (DSA).

## RESULT

The consumer is made more aware of counterfeit goods thanks to the introduction of a false product identification system. In blockchain technology, a serial number is generated using the ECDA algorithm by the manufacturer. The user then enters the produced serial number to verify the authenticity of the product.

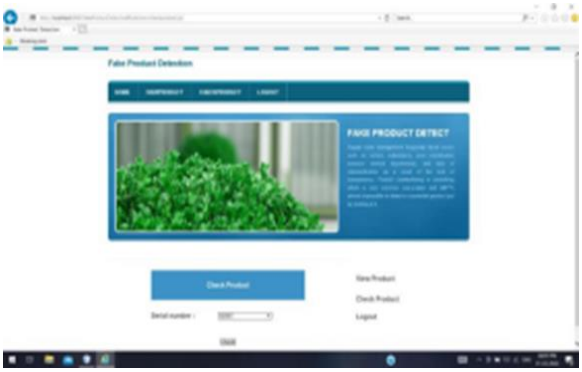

Fig.6. Customer Login Page

Fig.7 Real Product

© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 10 , Issue : 02 | April - June 2023

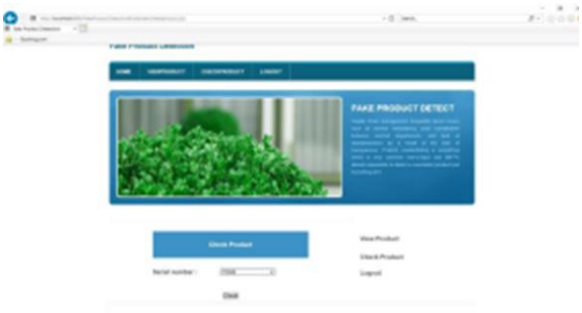

Fig.8 Checking the Product

Fig. 9 Fake Product Detected

## CONCLUSION AND FUTURE ENHANCEMENT

It was suggested to implement a Blockchain-based anti-counterfeit management system for fake goods. In this paper, we present a system architecture for integrating blockchain and supply chains, including in-depth analyses and explanations of all supply chain processes. The goods and methods are recorded on the blockchain network to provide clients simple anti-counterfeiting tracking of their purchases. The unlawful section of the supply chain may be checked without much effort using the third-party arbitration method. All involved in manufacturing as well as end users are afforded sufficient safety.

The whole system is encrypted using the Elliptic Curve Digital Signature Algorithm (ECDSA). To protect the confidentiality, authenticity, and integrity of the system's data, we used ECDSA to encrypt all communications throughout the supply chain. We also improved the safety of the system's data uploading operation and updates by deploying and constructing the chain code.

This system prioritises data security as compared to the contributions of other approaches. We refined the overall architecture and performed a thorough cryptographic analysis of the system's security. The communication study reaches the same conclusion, suggesting the system excels in this area as well.process. Blockchain is a decentralized system, Hence, the suggested method prevents local vendors from interfering with product verification or counterfeiting. Assuring the security and privacy of the data on the network, the system allows manufacturers and suppliers to record product information in Blockchain, which has tamper-resistance, data consistency, and secrecy. The client may check the authenticity of the goods by seeing its origins in the supply chain. Products sold to consumers are guaranteed to be free of defects. The suggested method has the potential to significantly reduce the prevalence of counterfeiting of branded goods and offer enterprises with a simpler means of assuring customers that they are not buying fake products. In addition to boosting the economy and minimising instances of corruption, this approach will assist to foster trust and strengthen relationships between businesses and their customers. More infrastructure is needed to prevent fraud in financial services, healthcare, elections, e-commerce, and other industries.

## REFERENCES

[1] "ASPA, The state of counterfeiting in india 2021, https : / / www.aspaglobal.com / pre_upload / nation / 1623216858-4730baa0efdb83aba174859af0a3a6a5-Report % 20The % 20State % 20of % 20Counterfeiting % 20in % 20India % 202021.pdf (2021)

[2] Y. Lu, Journal of Management Analytics 5, 1 (2018)

[3] F. Casino, T.K. Dasaklis, C. Patsakis, Telematics Informatics 36, 55 (2019) [4] M. Peck, IEEE Spectrum 54, 26 (2017)

[5] S. Idrees, M. Nowostawski, R. Jameel, A. Mourya, Electronics 10, 951 (2021)

[6] Zignuts Technolab, How blockchain architecture works? basic understanding of blockchain and its architecture., https : / / www.zignuts.com / blogs/how blockchain-architecture- works basic understanding- of-blockchain- and its- architecture/ (2022)

[7] J. Ma, S.Y. Lin, X. Chen, H.M. Sun, Y.C. Chen, H. Wang, IEEE Access 8, 77642 (2020)

[8] M.J.L.M.J.M. Bohli, N. Gruschka, IEEE 10, 9 (2013)

[9] C. Shaik, Computer Science & Engineering: An International Journal (CSEIJ) 11 (2021)

[10] M.A. Benatia, D. Baudry, A. Louis, Journal of Ambient Intelligence and Humanized Computing pp. 1–10 (2020)

[11] G. Khalil, R. Doss, M. Chowdhury, IEEE Access 8, 47952 (2020)

[12] M.A. Habib, M.B. Sardar, S. Jabbar, C.N. Faisal, N. Mahmood, M. Ahmad, Blockchain-based supply chain for the automation of transaction process: Case study based validation, in 2020 International Conference on Engineering and Emerging Technologies (ICEET) (IEEE, 2020), pp. 1–7

[13] E. Daoud, D. Vu, H. Nguyen, M. Gaedke, Improving Fake Product Detection Using Ai-Based Technology, in 18th International Conference e-Society (2020)

[14] S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, J. Zhang, A blockchain-based supply chain quality management framework, in 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE) (IEEE, 2017), pp. 172–176

[15] K. Toyoda, P.T. Mathiopoulos, I. Sasase, T. Ohtsuki, IEEE access 5, 17465 (2017)

[16] M. Nakasumi, Information sharing for supply chain management based on block chain technology, in 2017 IEEE 19th conference on business informatics (CBI) (IEEE, 2017), Vol. 1, pp. 140–149

[17] G. Wood et al., Ethereum project yellow paper 151, 1 (2014)

[18] A. Ghadge, A. Duck, M. Er, N. Caldwell, Supply Chain Forum: An International Journal 22, 87 (2021), https://doi.org/10.1080/16258312.2021.1908844

[19] I. Singhal, International Journal for Research in Applied Science and Engineering Technology 9, 291 (2021) [20] Chin-Ling Chen, Xin Shang, Woei Jiunn Tsaur , Wei Weng,, Yong-Yuan"