

High Secured Data Access and Leakage Detection Using Attribute-Based Encryption



Mercy Paul Selvan, Repala Sai Sowmith, Puralasetti Dheeraj, and S. Jancy

Abstract Brilliant innovations within reach have encouraged age and assortment of immense volumes of information, on regular schedule. It includes exceptionally touchy and differing information like individual, authoritative, condition, vitality, report, and personal information. Information analytics give answer for different issues being looked by brilliant hospital information like emergency reaction, debacle versatility, rise the executives, doctors, the executives framework, and so on. It requires conveyance of delicate information among different elements inside or outside the hospital. Sharing of touchy information makes a requirement for effective utilization of brilliant hospital information to give savvy applications and useful to the end users in which are liable and experimental method. This mutual delicate information if gets piled as an outcome can make harm and extreme hazard the hospital assets. Strong hold of basic information from informal exposure is greatest issue for accomplishment of any task. Information leakage perception gives a lot of instruments and innovation that can productively settle the worries identified with patient basic information. The principle goal of this task is to identify the guilty operator/individual who are indented to hack the information. We additionally send blockchain idea over this undertaking for high security. We give fake/copy record to those liable individual.

Keywords Big data · Blockchain · Data analytics · Data leakage · Hospital

M. P. Selvan (✉) · R. S. Sowmith · P. Dheeraj · S. Jancy
Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India
e-mail: mmercypaulselvan@gmail.com

R. S. Sowmith
e-mail: Indiarsaisowmith@gmail.com

P. Dheeraj
e-mail: dheeraj1332@gmail.com

S. Jancy
e-mail: jancymtech11@gmail.com

1 Introduction

Cloud computing offers an assorted scope of re-appropriating administrations, including capacity and calculation to serve people and endeavors. Essentially, redistributing administrations as a rule incorporate online installment and security issues. Be that as it may, most customary assistance arrangements need to depend on a trusted third party to acknowledge reasonableness to finish installments. For instance, Google cloud stage offers an assortment of processing administrations, for example, information stockpiling and calculation, and the client enrollment, and administration utilization needs a ledger made by an outsider budgetary foundation [1]. This can prompt major issues, for example, arrange interference when banking frameworks are out of administration or information spillage brought about by the cloud outsider. In this manner, the acknowledgment of secure and reasonable installment of re-appropriating administrations is of central significance for cloud-based applications. Right now has risen as a solid possibility to understand security issues of cloud administrations on account of its conveyed and unchanging natures. The works present a blockchain-based reasonable installment to the design for using redistributing administrations in cloud computing. The proposed framework guarantees to give adequacy and hearty decency capacities by utilizing an assistance the board convention run by blockchain. Reasonable installment can be accomplished among clients and re-appropriating specialist organizations on mists through exchanges which are put away and confirmed by blockchain without the contribution of any outsider. The development in the correspondence innovation has encouraged the associations to track about every single movement or occasion happened inside its premises. Enormous information essentially doesn't mean immense volume of information gathered through sensors; however, it is the information accessible to be examined utilizing propels apparatuses to bless savvy and to a hospital by deciding patterns, openings, and different dangers related [2]. A hospital owing canny framework as far as social, financial, and physical framework is considered as keenone [3, 4]. The most critical worry about the keen hospital private information at present is the issue of information rupturing which restricts the protection and safety of essential information. This huge volume of delicate key information is needed to be shielded from information leakages [5]. Previous situation of quick development requires the sharing of touchy information of element among assorted partners inside or outside the association (here hospital) premises for examining reason [6, 7]. However, the accepting substance may abuse this information and can spill it intentionally or unintentionally to some unapproved outsider [8, 9]. Information spillage is characterized as the thought or inadvertent dispersion of touchy data or information to an unapproved vindictive element [10]. Basic information in different associations as appeared in Fig. 1 [11] incorporate Intellectual Property (IP), segment data, foundation subtleties, open area information, monetary data, and different other data relying on the hospital [12]. Information spillage uncovered a major test and extraordinary danger to the association privacy in light of the fact that as the include of breaks increments in resultant the expense happened because of these spillages likewise

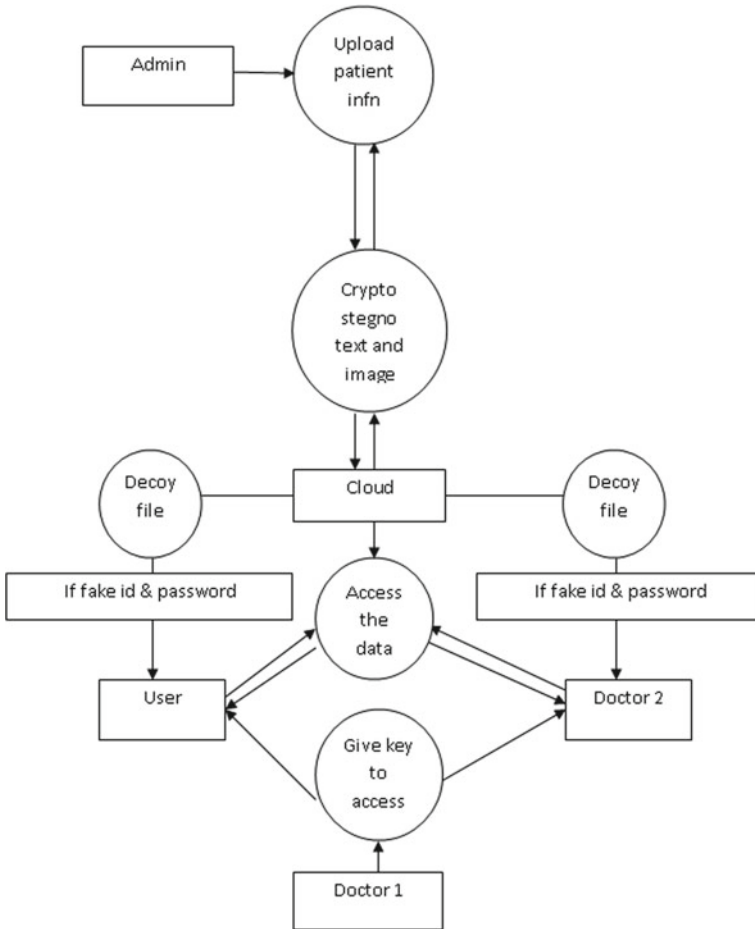


Fig. 1 Proposed system architecture

keep on expanding [13, 14]. It is fundamental to ensure the private data as it builds the danger of falling the touchy data in unapproved hands, and afterward, it tends to be abused by unapproved outsider [15, 16]. Accordingly, it has gotten basic for any association to identify and forestall such spillage [17]. Therefore, if limit the information sharing to control security and protection of delicate data may decrease the association’s development [18]. The customary methodology like watermarking, steganography for the information spillage recognition includes alteration in the first information [19, 20] so while another, a model to distinguish the malignant guilty operator who caused spillage of basic data and gives security to shield the touchy data [21]. This representation visualizes the blameworthy operator by watching the example of information assignment among different specialists. In the model, wholesaler dispenses the mentioned information thing among different specialists, spoke

to through bi-graph. In the wake of accepting the pivotal information, if specialist uncovers this information to some noxious outsider, and at some point, later information is discovered be extant at some unapproved place; system to recognize spillage is utilized to disclose the datasp.

2 Related Work

Numerous examinations in Cloud of Things, blockchain, and related issues have been explored over the ongoing years in a wide scope of specialized angles. Numerous endeavors have been made to give survey articles on this examination territory in various degrees. The overview papers displayed the audit of late endeavors in the appropriation of blockchain innovation in different cloud situations and applications [22, 23]. They additionally dissected specialized parts of blockchain–cloud mixes, from definition, coordinated structures, empowering advancements to application situations and open issues. In the interim, the creators talked about research [24].

Issues, difficulties, and chances of mix among blockchain and cloud computing. They concentrated on the upsides of blockchain reception in cloud systems, including security, information the executives, and application areas with potential help stages. The work introduced a review on the utilization of the blockchain innovation to give security administrations, and its specialized properties to tackle related difficulties in different application spaces, including cloud processing. All the more as of late, the review on the incorporated model of blockchain and edge figuring, an all-inclusive cloud computing idea, was talked about in the study [25].

We propose an appropriated, versatile and fine-grained get to control conspire with proficient decoding for the big data in mists. Blockchain innovation is utilized to oversee personalities and give the validation, store, and execute a shrewd agreement that consolidates the relevant and nitty gritty access arrangement characterized by the information proprietor, which is activated by an entrance requester that gives information proprietors the sovereign right to successfully deal with their informational collections and deals with the strategy. We additionally utilized the ciphertext-policy attribute-based encryption plot for supporting the effective decoding re-appropriating as another security layer for dealing with the arrangement.

In a CP-ABE plot, every client's key is related with properties, and each ciphertext is identified with an entrance arrangement; therefore, information proprietors can decide the entrance approaches for their own information and control them straightforwardly. In the event that a client's (patient) traits fulfill the entrance arrangement in the cipher text, the client can decode the cipher text effectively. In addition, CP-ABE has an integral framework called key strategy Attribute-Based Encryption (KPABE) [14]; in which every client's key is related with an entrance arrangement, and each ciphertext is determined with traits [26]. The utilization of CP-ABE to the cloud condition can bring information spillage anticipation and gain control together, which are structural essentials for big data security and protection [2].

Most access control arrangements receive an incorporated engineering. They redistribute the control of information to confided in outsiders, which keep the client from controlling his own information. This can cause issues of morals and classification. Lamentably, when we share our data with outsiders, we promptly lose control and possession. Our new plan official breaks this custom and gives individuals what has a place with them in a reasonable manner. Truth be told, we accept that big data needs an other entrance control structure that meets its particular prerequisites and highlights, permitting clients to control their own protection. This “change” will require reexamining access control advances and making another arrangement that tends to the security and protection prerequisites of big data. Ideally, we are on the edge of another period of decentralization, which has brought another innovation, known as blockchain, that could change in a general sense our thoughts of incorporated position.

3 Existing System

There is no framework to distinguish the guilty specialist/individual; there is no security to keep away from information spillage of delicate data. Existing situation of quick development requires the sharing of delicate information of substance among assorted partners inside or outside the association (here hospital) premises for examining reason. Be that as it may, the accepting element may abuse this information and can spill it intentionally or accidentally to some unapproved outsider. Information spillage is characterized as the pondered or unintentional conveyance of touchy data or information to an unapproved malevolent substance.

4 Proposed System

It includes profoundly delicate and differing information like individual, authoritative, condition, vitality, transport, and financial information. Information analytics give answer for different issues being looked by savvy urban communities like emergency reaction, debacle versatility, development the executives, keen patients the board framework, and so on. It requires conveyance of touchy information among different elements inside or outside the hospital. Sharing of those delicate information is troublesome and hard. We embrace information spillage identification framework to distinguish the guilty operator/individual. In the proposed piece of work, we distinguish the guilty specialist/individual through wrong passwords based confirmation. When our framework recognizes the blameworthy individual at that point fake document/wrong record is disseminated to that programmer. All the information is put away utilizing blockchain innovation for high security reason. All the information is put away in cloud server for viable remote access.

4.1 User Registration

Right now/persistent need to enlist their own data like name, address, mail ID, portable number, address. What's more, those subtleties will be put away on database. After enlistment, client will get client ID and secret key to get to the application. This is an application to see their emergency clinic report from cloud. To get to the emergency clinic records, we are making client Id and secret word for confirmation.

4.2 Hospital Server

Server is the principle procedure for each application since it is the main path for correspondence it will build up the correspondence among customer and relating site. Right now are executing emergency clinic server to keep up both patient data, specialist data, and other medical clinic subtleties. All specialists need to enroll their assignment and different subtleties same like that other medical clinic need to enlist their subtleties on this server. Since patient may change their treatment starting with one medical clinic then onto the next that is the reason emergency clinic will like wise enroll their data. Server will keep up all the subtleties and give subtleties at whatever point client solicitation to the inquiry (Figs. 2 and 3).

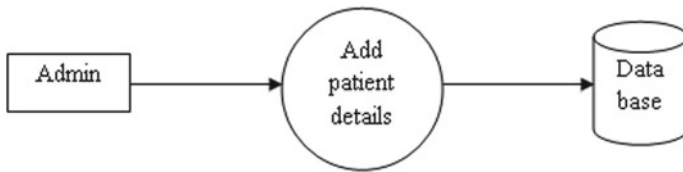


Fig. 2 User registration



Fig. 3 Hospital server

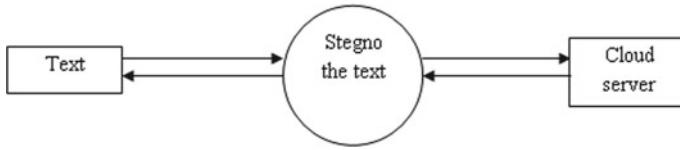


Fig. 4 Stegno analysis

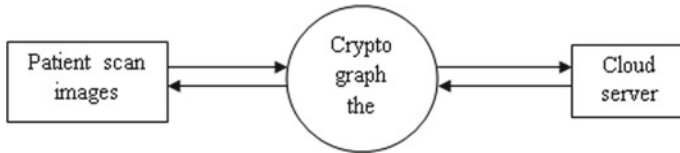


Fig. 5 Image cryptography

4.3 Stegno Analysis

Steganography is the method of concealing personal data (record, message, picture, or video) inside another document, message, picture, or video. We are concealing the patient’s close to home data and their report about sickness. Each datum will be put away as a stegno position at the point when we put away the record as a stegno it won’t hacked or burglary by any one (Fig. 4).

4.4 Image Cryptography

In our framework, we are putting away the patient filtering report like the irx-beam, ECG, and different pictures in scrambled structure utilizing ECC calculation. ECC produces keys through the properties of the elliptic bend condition rather than the customary strategy for age as the result of exceptionally enormous prime numbers. Utilizing ECC calculation, we are scrambling the picture document and store it in cloud server (Fig. 5).

4.5 Fog Computing

Haze figuring is a term made by Cisco that alludes for developing of cloud computing to the edge of an undertaking’s system. Otherwise said the edge computing or misting, haze transforming boosts the activity of register, stockpiling, and systems administration benefits between end apparatus and cloud computing server warehouses. It is a different to keep up the distraction data. Here, we fake the patient data in secure

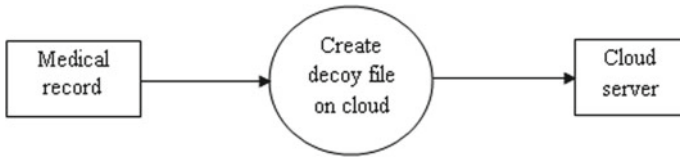


Fig. 6 Fog computing

manner that is the way to ward making aphony report of patient. For security, we are making this kind of record (Fig. 6).

4.6 Data Access

Right now are actualizing getting to process for client just as emergency clinic. Right now, tolerant detail will be kept up by a specialist who is the individual patient met from the outset time. He had just authorization to get to the patient data. On the off chance that it any case understanding change the emergency clinic or he/she needs to see his/her subtleties that they need some key to get to the information which is put away in cloud. In the event that the patient their clinic another specialist need to offer key to get to the patient subtleties. For the two individuals, they need one key to get to the document. That key will be given by specialist from emergency clinic. Both patient and specialist have client id and secret phrase to get the document. Framework will check their ID and secret expression on the off chance that it coordinate with past information nbase, and they will get key from specialist and view subtleties. In the event that it won't coordinate with past database server which will give distraction record, and ready will be send to the patient (Fig. 7).

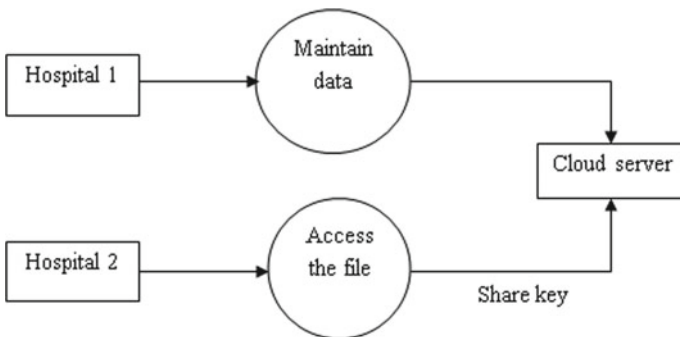


Fig. 7 Data access

4.7 ABE Implementation

Attribute-Based Encryption (ABE) may be used to encrypt files. Rather of encrypting each part of a log with the keys of all recipients, the log can only be authenticated with attributes that suit attributes of the recipients. This basic can also be used to encrypt transmissions and reduce the amount of keys used. The multiple applications can view all the patient data like doctors, technicians [27], and nurses depending on their consent to view them and their keys.

4.8 Blockchain Implementation

A square is a compartment information configuration. The normal size of a square is by all accounts 1MB (source). Here, each testament number will be made as a square. For each square, a hash code will process for security.

5 Result and Steps

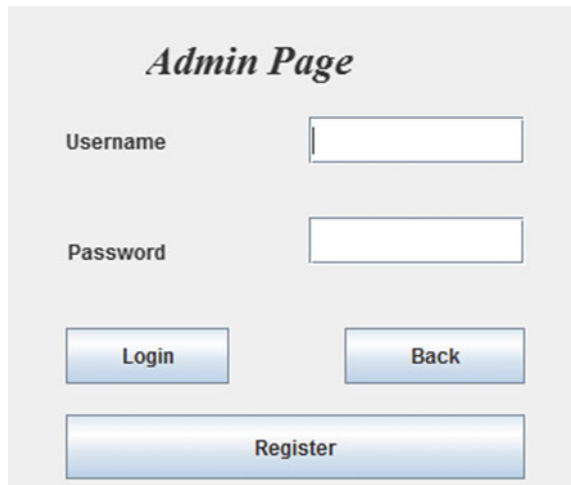
Step 1 (Fig. 8):

Step 2 (Fig. 9):

Step 3 (Fig. 10):

Step 4 (Fig. 11):

Fig. 8 Admin page



The image shows a web form titled "Admin Page". It contains two input fields: "Username" and "Password". Below these fields are three buttons: "Login", "Back", and "Register". The "Login" and "Back" buttons are positioned side-by-side, while the "Register" button is centered below them.

Fig. 9 User registration

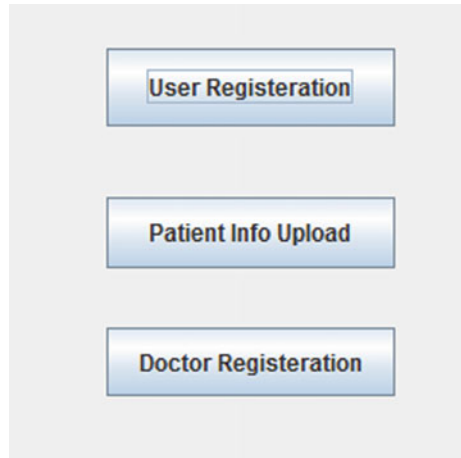


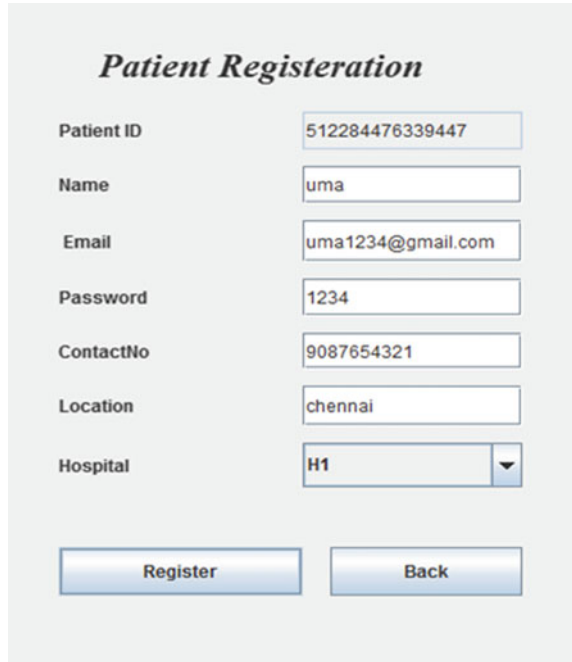
Fig. 10 Patient registration

Patient Registration

Patient ID	<input type="text" value="512284476339447"/>
Name	<input type="text"/>
Email	<input type="text"/>
Password	<input type="text"/>
ContactNo	<input type="text"/>
Location	<input type="text"/>
Hospital	<input type="text" value="H1"/> ▼

- Step 5** (Fig. 12):
- Step 6** (Fig. 13):
- Step 7** (Fig. 14):

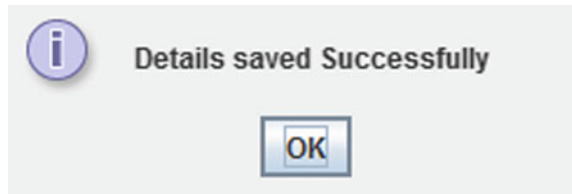
Fig. 11 Patient details



Patient Registration

Patient ID	<input type="text" value="512284476339447"/>
Name	<input type="text" value="uma"/>
Email	<input type="text" value="uma1234@gmail.com"/>
Password	<input type="text" value="1234"/>
ContactNo	<input type="text" value="9087654321"/>
Location	<input type="text" value="chennai"/>
Hospital	<input type="text" value="H1"/>

Fig. 12 Saving details



6 Conclusion

Brilliant hospital is information driven enormous information gathered by omnipresent shrewd things like different medicines, various medical report, and so forth change the lives of occupants by benefiting an a lot of savvy and clever applications and help in dynamic capacity. Effective execution of hospital idea relies upon the productive utilization and security of touchy information. Given model takes care of information spillage issue utilizing a blame operator distinguishing proof model to recognize the spillages that are caused deliberately or accidentally. It finds the odds of the operator for being blameworthy by processing likelihood relying upon the information dispensed among different specialists through bi-graph. Data leaker is recognized by contrasting the determined likelihood of releasing the information, and the classified data is safeguarded. Future endeavors could be made to improve the security of the most delicate data by means of considering the edge esteem.

Patient Info

Patient ID: 512284476339447

Disease: cancer

Do: 500ml

Do: doc1

Ho: H1

ReC:\Users\Sathish digital\Pictures\download.jpg

Image File:- download.jpg

Content File:- cert.txt

Fig. 13 Patient documents updation



Fig. 14 Patient report

References

1. Gupta, I., & Singh, A. K. (2018). A probabilistic approach for guilty agent detection using bigraph after distribution of sample data. *Procedia Computer Science*, 125, 662–668.
2. Shu, X., Zhang, J., Yao, D., & Feng, W. C. (2016). Fast detection of transformed data leaks. *IEEE Transactions on Information Forensics and Security*, 11(3), 528–542.
3. Mounnan, O., & Abouelkalam, A. (2019). Efficient distributed access control using blockchain for big data in clouds. In *ICWMC 2019: The Fifteenth International Conference on Wireless and Mobile Communications*.
4. Sharif, A., Li, J., Khalil, M., Kumar, R., & Sharif, M. I. (2017). Internet of Things-smart traffic management system for smart cities using big data analytics. In *IEEE* (pp. 281–284).
5. Xu, C., Huang, X., Zhu, J., & Zhang, K. (2018). Research on the construction of sanya smart tourism city based on internet and big data. In *International Conference on Intelligent*

- Transportation, Big Data & Smart City* (pp. 125–128).
6. Papadimitriou, P., & Molina, H. G. (2011). Data leakage detection. *IEEE Transaction on Knowledge and Data Engineering*, 23(1), 51–63.
 7. Croft, J., & Caesar, M. (2011). Towards practical avoidance of information leakage in enterprise networks. In *6th USENIX conference Hot Topics Security (HotSec)*, CA, USA (p. 7).
 8. Kaur, K., Gupta, I., & Singh, A. K. (2017). A comparative evaluation of data leakage/loss prevention systems (DLPS). In *4th International Conference on Computer Science & Information Technology (CS & IT-CSCP)*, Dubai, UAE (pp. 87–95).
 9. Backes, M., Grimm, N., & Kate, A. (2014). Lime: Data lineage in the malicious environment. In *10th International Workshop Security Trust Management* (pp. 183–187).
 10. Kumar, A., Goyal, A., Kumar, A., Chaudhary, N. K., & Kamath, S. (2013). Comparative evaluation of algorithms for effective data leakage detection In *IEEE Conference on Information and Communication Technologies (ICT 2013)* (Vol. 13, pp. 177–182).
 11. Sholla, S., Naaz, R., & Chishti, M. A. (2018). Semantic smart city: Context aware application architecture. In *2nd International Conference on Electronics, Communication and Technology (ICECA)* (pp. 721–724).
 12. Waters, B. (2011). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *PKC' II* (pp. 53–70).
 13. Shu, X., & Yao, D. (2012). Data leak detection as a service. In *Springer, International Conference on Security and Privacy in Communication Systems* (pp. 222–240).
 14. Liu, F., Shu, X., Yao, D., & Butt, A. R. (2015). Privacy-preserving scanning of big content for sensitive data exposure with MapReduce. In *5th ACM Conference Data Application Security, Privacy (CODASPY)*, Texas, USA (pp. 195–206).
 15. Gafny, M., Shabtai, A., Rokach, L., & Elovici, Y. (2010). Detecting data misuse by applying context-based data linkage. *ACM Workshop Insider Threats* (pp. 3–12).
 16. Kaur, K., Gupta, I., & Singh, A. K. (2017). A comparative study of the approach provided for preventing the data leakage. *International Journal of Network Security & Its Applications*, 9(5), 21–33.
 17. Shu, X., & Yao, D. (2015). Privacy-preserving detection of sensitive data exposure. *IEEE Transactions on Information Forensics and Security*, 10(5), 1092–1103.
 18. Harel, A., Shabtai, A., Rokach, L., & Elovici, Y. (2012). M-Score: A miuseability weight measure. *IEEE Transactions on Dependable and Secure Computing*, 9(3), 414–428.
 19. Gupta, K., & Kush, A. (2017). A review on data leakage detection for secure. *International Journal of Engineering and Advanced Technology (IJEAT)*, 7(1), 153–159.
 20. Gupta, K., & Kush, A. (2018). Performance evaluation on data leakage detection for secure communication. In *5th International Conference on "Computing for Sustainable Global Development: INDIACom*, New Delhi, India (pp. 3957–3960).
 21. Viji Amutha Mary, A., Selvan, M. P., Christy. (2019). Public auditing for secure cloud storage using MD5 algorithm. *International Journal of Recent Technology and Engineering (IJRTE)*, 8(3).
 22. Viji Mary, A. (2018). A novel technique to secure the acute myocardial infarcta images by the enhancement of privacy level.
 23. Mala, G. A. (2013, December). Tracking international migration from RFID data using map reduce method. In *2013 Fifth International Conference on Advanced Computing (ICoAC)* (pp. 484–487). IEEE.
 24. Minu, R. I., Nagarajan, G., & Pravin, A. (2019). BIP: A dimensionality reduction for image indexing. *ICT Express*, 5(3), 187–191.
 25. Jacob, T. P. (2015). Implementation of randomized test pattern generation strategy. *Journal of Theoretical and Applied Information Technology*, 73(1).
 26. Kajendran, P., & Pravin, A. (2017). Enhancement of security related to ATM installations to detect misbehavior activity of unknown person using video analytics. *ARPN Journal of Engineering and Applied Science*, 12(21).
 27. Rajendran, P. K., Muthukumar, B., & Nagarajan, G. (2015). Hybrid intrusion detection system for private cloud: a systematic approach. *Procedia Computer Science*, 48(C), 325–329.