iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 11 **Issue:** VII **Month of publication:** July 2023

**DOI:** https://doi.org/10.22214/ijraset.2023.55016

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 11 Issue VII Jul 2023- Available at www.ijraset.com*

# Security Analysis on Surveillance System

Dr. Sowmyarani C N[1], Lavanya Naik[2], Sangeetha S[3]
[1]*Associate Professor, Dept of CSE, RV College of Engineering, Bangalore*
[2, 3]*M.Tech in Computer Network Engineering, Dept of CSE, RV College of Engineering, Bangalore*

***Abstract:*** ***Nowadays in every organization, office, home, shops it has become mandatory to have surveillance system. This is for safety purpose in order to avoid theft and in turn achieve security. Most of the surveillance systems are managed and monitored by third parties as they are the ones who distribute them to various organizations. Meanwhile in some cases, for example in hospital, patient's data might be sent to third parties in order to find best diagnosis or medicines for the disease that is increasing.***
***In such cases there are high chances that these data are stolen from third parties, or third parties might send those data to some unauthorized users. This might lead to misuse of data. Therefore, one of the main security threats to surveillance system is data leakage. Data leakage prevention is becoming increasingly important as more and more data is generated. In this paper, system is designed which gives clear idea on who are the third parties for whom data is sent and who are those leakers who are misusing those files and block them or report them.***
***Keywords: data leakage, authentication, security, surveillance system.***

## I. INTRODUCTION

Earlier to look after something that is very important, there were watchmen kept at that place to look after things. This indeed did not do much needful work as there were risk of theft even after this. But with the growth of technology there was alternative option chosen to make sure there is eye kept on those important things, or important place, etc. This alternative option is installing surveillance cameras in that location so that surrounding is under observation. This makes an advantage that there is no need to for any person to physically being present there.
These surveillance systems are recorded so that if there is something missing then, one can go check the recordings. This would make them easy to find out who is culprit. But if there is security issues for surveillance systems only then it becomes difficult. Because the surveillance systems are controlled or bought from third parties, there is security threat. Major Security threat is "data leakage". Consider hospital scenario, wherein patient's data is sent to some third party like pharmaceutical company for diagnosis of the newly found disease and find the medicines or treatments for the same. Then there might be some other third party who steals that data or any person leaks the data which is judicially not right, then identifying those leakers and taking right actions on them is required. So this report explains on how data leakage can happen, ho to detect those leakages and take actions on that leakers

## II. LITERATURE SURVEY

In [1], author considers a scenario where distributor sends files to set of agents and identifies that the files sent to these trusted parties are found in internet and is being leaked. So author builds a guilty agent model to find who is that agent leaking files or sending to some other unauthorized people. But to claim that agent is guilty probability check is made and finally decided as guilty and those guilty agents are blocked. So measure taken here is to watermark the data that is sent so that it is easily identified even if it gets leaked. In [2], Every application now are built on cloud for its vast advantages of pay as you go, scalability, availability at any time, reduction of infrastructural cost. But it comes with disadvantage of secure as third parties can get access if they get access to cloud. In this paper author uses Smax algorithm, finds the guilty agent. Here probability is calculated for agents that who has high probability of leaking the files.
In [3], author provided a new method to identify leaked documents. This is done by giving time stamp to each document. Time stamp is attached for every file to give permission in order to access the file. Only for the period of that timestamp the document is considered to be confidential. Once this is crossed, document is considered to be non-confidential, and this prevents data leakage. Author claims that using this approach one can find data is confidential or not and avoid 100% data leakage prevention. Systematic Literature Review on real-time privacy-preserving video surveillance [4] is conducted. In this paper author a framework in order to preserve privacy by storing the encrypted version of data that comes out of surveillance system. This is mainly applied for recognition of face and number plates in traffic surveillance cameras.

Author in paper[5] discusses on what are all the root causes of attacks on surveillance cameras. Model is proposed by author in order to find out vulnerabilities which exploits the trust on the surveillance cameras. Author finds out if the data sent from the feed is corrupted due to ddos attack or man in the middle attack. In [6], author proposes model to address current security threats and weakness of IOT systems. Users of these system used internet to control connect to respective machines. The main motivation is the vulnerabilities that in IP cameras. Inspection is done directly on few IP cameras and analysis is made on what are all the flaws and weakness that are in IP cameras.

## III. MOTIVATION

The main motivation behind the project is the need for data security is increasing day by day. The need for monitoring public and private areas is gaining due to persisting security reasons. A Surveillance security system that provides automatic analysis of data and several features added to enhance the monitoring performance and to eliminate possible human failures. The project "Security analysis in Surveillance sysyems" analyzes different kinds of attacks on surveillance system and to perform security analysis and techniques to overcome data leakages in surveillance system.

## IV. METHODOLOGY

Man In The Middle Attack is the first vulnerability addressed. ARP spoofing is used as the first step in this attack. Every computer has ARP address which has records of all MAC address and all IP addresses. If there is no proper checks at this table end, there might vulnerability attack. Integrity violation is a process of blocking data and simultaneously fooling that data is alive to victim. This is done by collecting samples of images from camera and then send those images in loop

The methodology of the project are stated as follows:

*1)* Validation of user based on the credentials
*2)* Based on the role, redirect to their operations.
*3)* Distributor sends the file to group of agents by encrypting the files using secret key algorithm.
*4)* Agent who gets the notification of new file, opens the file if he has secret key
*5)* Else agent requests for key to decrypt file
*6)* Distributor gets notified who all downloaded the file
*7)* If there is any unauthorized person accessing file, that person is blocked
*8)* And also check which agent has leaked file and report that agent
*9)* The claimed guilty agent's access is revoked thereby detecting and stopping data leakage.

The text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

## V. DESIGN

The proposed methodology will identify the data that is leaked and all the leakers who have leaked the data. The admin who has complete control over the web application is able to check who are all the leakers and the files that is being leaked. enter the secret key that is shared only between the sender and receiver. If the receiver doesn't have the secret key he can request the sender for the same. Now sender will send request if the request is from dedicated receiver. After this key is received at receiver end, he can download the file using that key. If there is any other person

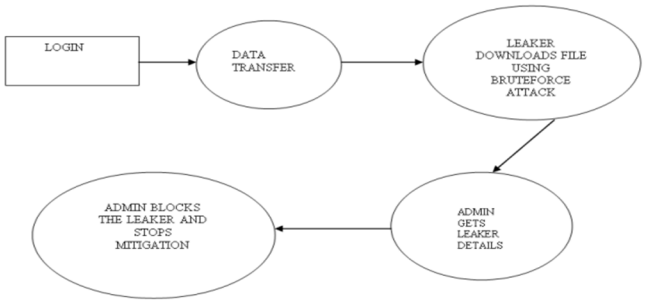



Fig 1: High level Design

Downloaded the file except the receiver, by somehow finding the key using brute force attack or man in the middle attack, then this is notified to admin at his dashboard. By doing this leaked file and leaker details is displayed at admin. Now admin can either block or remove the user from accessing the web application. This is how mitigation of data leakage is prevented.

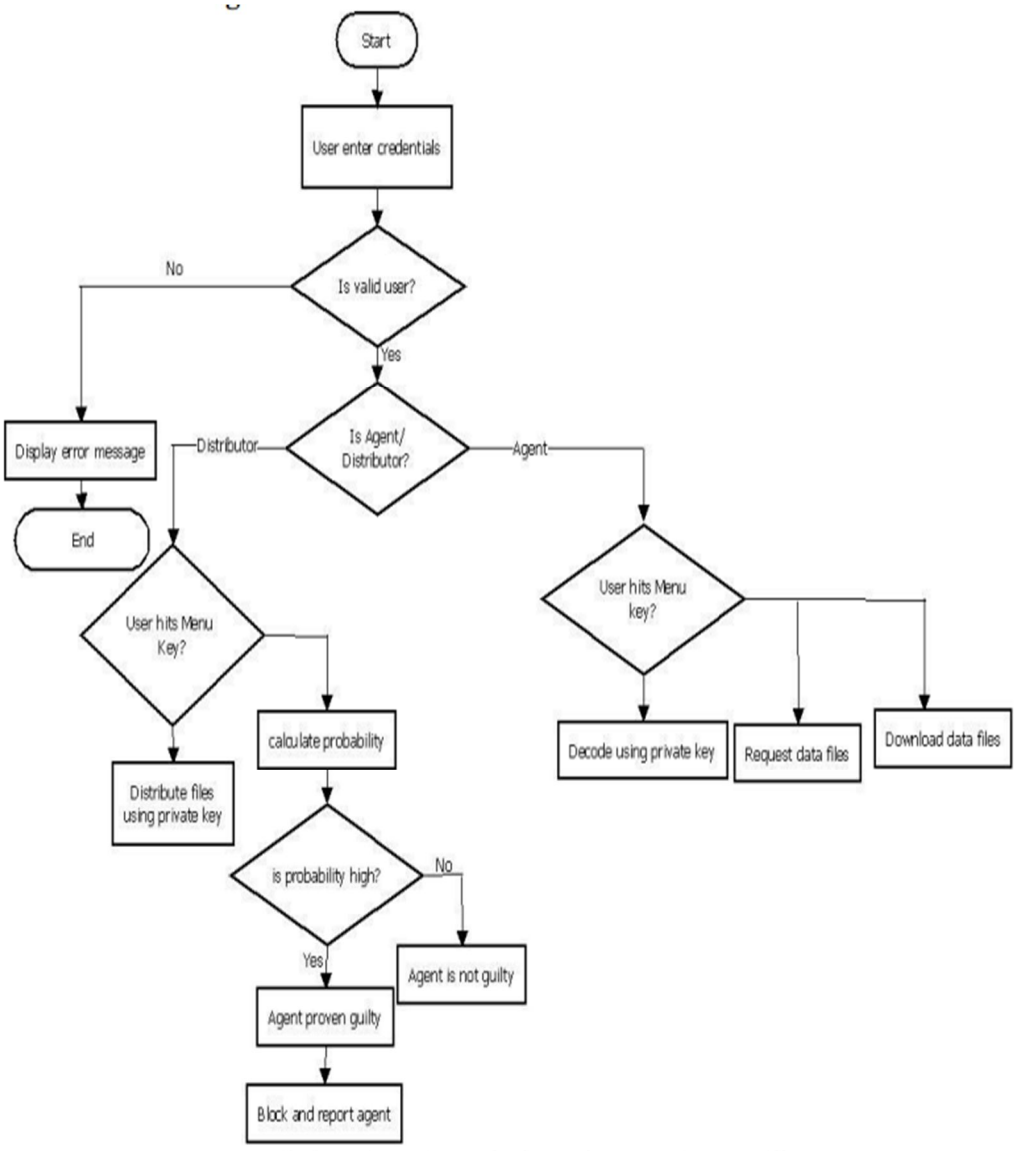



Fig 2: Detailed Design of Data leakage detection in surveillance system

*1)* Validation of user based on the credentials
*2)* Based on the role, redirect to their operations.
*3)* Distributor sends the file to group of agents by encrypting the files using secret key algorithm
*4)* Agent who gets the notification of new file, opens the file if he has secret key
*5)* Else agent requests for key to decrypt file
*6)* Distributor gets notified who all downloaded the file
*7)* If there is any unauthorized person accessing file, that person is blocked and also check which agent has leaked file and report that agent
*8)* The claimed guilty agent's access is revoked thereby detecting and stopping data leakage. To verify the product, user can either enter the product ID or scan the QR code.

## VI. IMPLEMENTATION

Details of newly registered user are sent to admin. Once admin login to his account, he finds the request. If he is valid user, then activate the user. This code checks if the user details is activated by admin. If yes, then user is given access to application the send or receive file. This is written using php language as shown in Fig 3

```
<?php
if(isset($_SESSION['is_login'])){
  if($_SESSION['is_login']=='loginned'){
?>
 <?php if(isset($_SESSION['profile'])){ ?>
        <li class="nav-item">
            <img src="assets/profiles/<?=$_SESSION['profile']?>" style="width: 40px; height:40px; border-radius: 100%;">
        </li>
       <?php } ?>
 <li class="nav-item">
   <a class="nav-link active" aria-current="page" href="views/dashboard.php"><?=strtoupper($_SESSION['username'])?></a>
 </li>
 <li class="nav-item">
   <a class="nav-link active" aria-current="page" href="views/logout.php">
     <i class="bi bi-box-arrow-right"></i> Logout</a>
 </li>
<?php }else{?>
 <li class="nav-item">
    <a class="nav-link active" aria-current="page" href="views/login.php"><i class="bi bi-box-arrow-in-left"></i> Login</a>
</li>
<?php }}else{?>
 <li class="nav-item">
   <a class="nav-link active" aria-current="page" href="views/login.php"><i class="bi bi-box-arrow-in-left"></i> Login</a>
 </li>
<?php }?>
```

Fig 3: Php code for validating user

```
<?php
 require_once("../session.php");
 require_once("../server/connect.php");
 $id=$_GET['id'];
 $asker=$_SESSION['user_id'];

 function getfiledetail($fileId){
 global $conn;
   $data="";
 $sql="SELECT * FROM data_files WHERE id='$fileId' LIMIT 1";
 $result=mysqli_query($conn,$sql);
 $row=mysqli_fetch_array($result);
 return $row;
 }

 $file = getfiledetail($id);
 $secret_key = $file['secret_key'];
 $request_to_user = $file['sender_id'];
 $sql="INSERT INTO key_requests(request_by_user, request_to_user, file, secret_key, status)VALUES('$asker', '$request_to_user', '$id', '$secret_key', 'pending')";
 mysqli_query($conn, $sql);
 echo "Request successfully sent.";
 ?>
```

Fig 4: PHP code to request key

Once the file is received in order to download the file, user needs to enter the key. To get this key receiver requests the sender using sender id. This request is sent at sender and using database the key is sent to receiver.

## VII. RESULTS

The results of this peper highlights the security analysis of surveillance system. Any video, image, document or file of any format sent between sender user and receiver user. If gets downloaded by any other user should be notified to admin and block the leaker

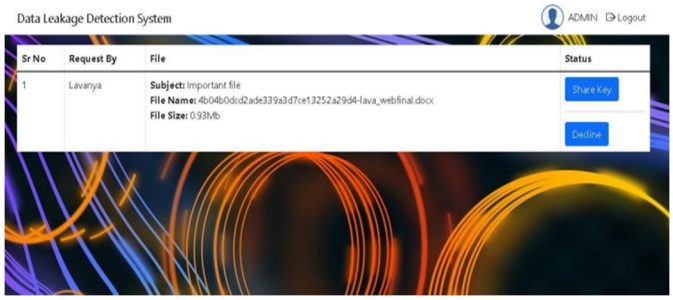



Fig 5: Admin getting key request from users

This figure[5] shows the key request sent by receiver in order to download the file that is sent by sender. Once the key request is received at sender, either send can chose to share key or to decline the request if it from unauthorized user.

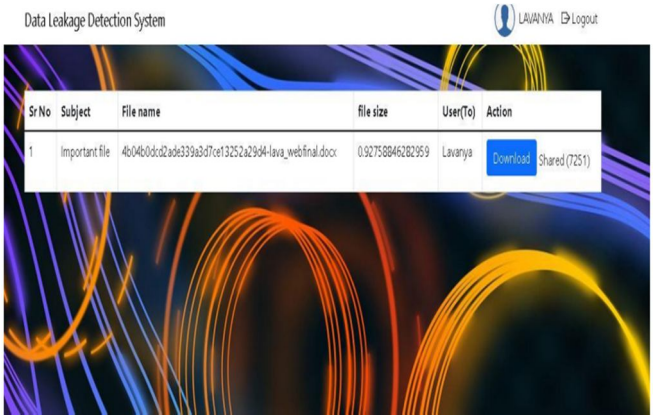



Fig 6: Key received at user end.

This figure[6] shows that the key is been shared from sender. Now receiver can see the shared key. Using this shared key user can download the file

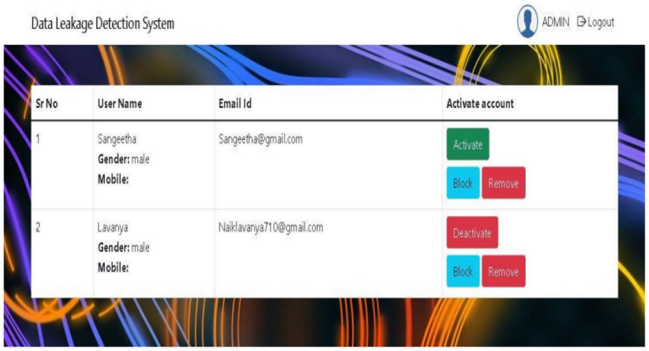



Fig 7: Admin getting request to activate new user

This figure[7] shows that every newly registered user request is sent to admin. Only if admin validates the user can login to the application

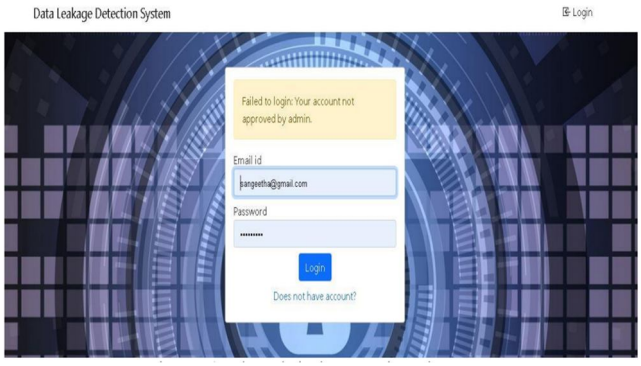



Fig 8: When admin doesn't activate the new user

This figure[8] shows that without admin activating the user account it is not possible. By this way only authenticate users can login to application

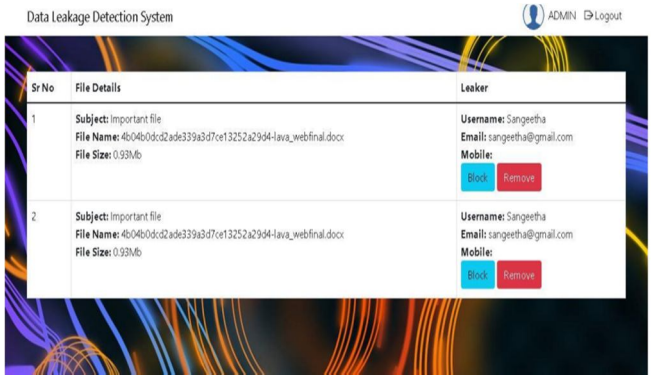



Fig 9: Leaker details displayed at admin's dashboard

Any user except the dedicated user, downloads the file sent by any user, then he is declared as leaker and the details of that leaker is sent at admin's dashboard as shown[9].

## VIII.CONCLUSION

Limitations of the project are as follows
Strong authentication: In this project we have used username and password as the login credentials. This is not very strong because if anyone gets to know username and password then they can access the files and download it.
Key generation system: The key that is attached to each file is some random 5 digit number. This is very easy to crack as only few number of combinations need to be tested. This in turn will lead to leakage as finding out this key using brute force

## IX. FUTURE WORK

Developing application in future and store all the details on cloud and deploy the application on cloud. Adding more security features like adding face recognition or biometric details before agent open file instead of just authenticating them by their login credentials. Using strong key generation and storing mechanism. The key that is attached to each file is some random 5 digit number. This is very easy to crack as only few numbers of combinations need to be tested. This in turn will lead to leakage as finding out this key using brute force. So use strong key generation algorithms like AED, DES etc. so that hacking this key would become very difficult and file is safe from attack.

## X. ACKNOWLEDGMENT

We are indebted to Rashtreeya Sikshana Samithi Trust, Bengaluru for providing us with all the facilities needed for the successful completion of our work at Rashtreeya Vidyalaya College of Engineering (RVCE) during the tenure of our course. We would like to thank Dr K N Subramanya, Principal, for giving us opportunity to be a part of RVCE and for his timely help and encouragement during the tenure of the work.

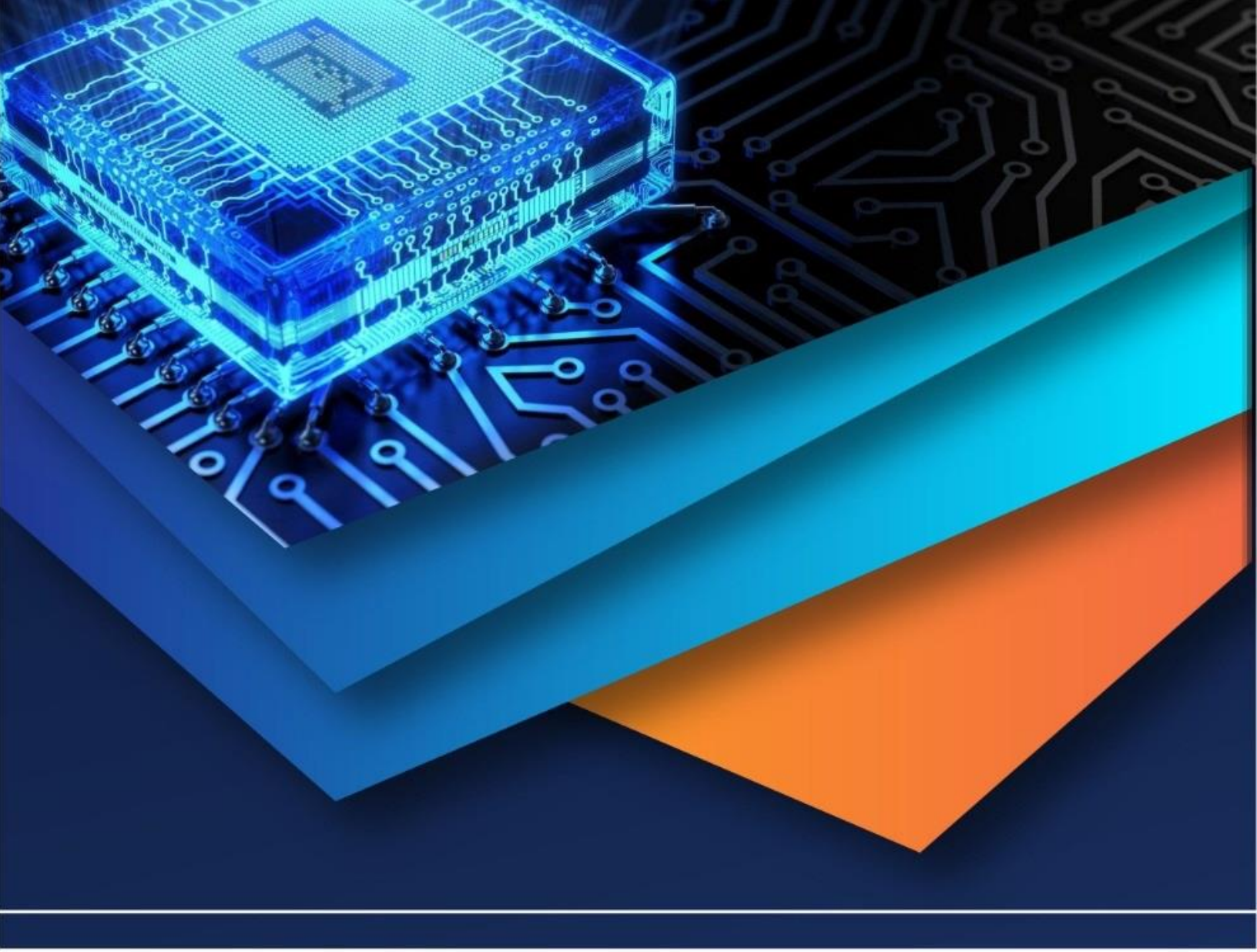
 

We are greatly thankful to Dr. Ramakanth Kumar, Professor and Head, Dept. of CSE for his motivation and constant support during the tenure of our work. We take this opportunity to convey our sincere gratitude to the guide Dr. Nagaraja G. S, Professor and Associate Dean, Dept. of CSE for his advice, support and valuable suggestions help us to accomplish the work in time. We extend our thanks to all who have directly or indirectly extended their constant support.

## REFERENCES

[1] Elharrouss, O., Almaadeed, N. and Al-Maadeed, S., 2021. A review of video surveillance systems. Journal of Visual Communication and Image Representation, 77, p.103116.
[2] Shidik, G.F., Noersasongko, E., Nugraha, A., Andono, P.N., Jumanto, J. and Kusuma, E.J., 2019. A systematic review of intelligence video surveillance: trends, techniques, frameworks, and datasets. IEEE Access, 7, pp.170457-170473.
[3] Lee, K., Yeuk, H., Kim, J., Park, H. and Yim, K., 2016. An efficient key management solution for privacy masking, restoring and user authentication for video surveillance servers. Computer Standards & Interfaces, 44, pp.137-143.
[4] P. Buneman and W.-C. Tan, "Provenance in Databases," Proc. ACM SIGMOD, pp. 1171-1173, 2018.
[5] Y. Cui and J. Widom, "Lineage Tracing for General Data Warehouse Transformations," The VLDB J., vol. 12, pp. 41-58, 2003.
[6] S.Czerwinski, R. Fromm, and T. Hodes, "Digital Music Distributionand Audio Watermarking," http://www.scientificcommons.org/43025658, 2017.
[7] Rahman, S.M.M., Hossain, M.A., Hassan, M.M., Alamri, A., Alghamdi, A. and Pathan, M., 2016. Secure privacy vault design for distributed multimedia surveillance system. Future Generation Computer Systems, 55, pp.344-352.
[8] Kim, J.S., Kim, M.G. and Pan, S.B., 2021. A study on implementation of real-time intelligent video surveillance system based on embedded module. EURASIP Journal on Image and Video Processing, 2021(1), pp.1-22.
[9] R. Agrawal and J. Kiernan, "Watermarking Relational Databases," Proc. 28th Int'lConf. Very Large Data Bases (VLDB '02), VLDB Endowment, pp. 155-166, 2019.
[10] Elharrouss, O., Almaadeed, N. and Al-Maadeed, S., 2021. A review of video surveillance systems. Journal of Visual Communication and Image Representation, 77, p.103116.
[11] Shidik, G.F., Noersasongko, E., Nugraha, A., Andono, P.N., Jumanto, J. and Kusuma, E.J., 2019. A systematic review of intelligence video surveillance: trends, techniques, frameworks, and datasets. IEEE Access, 7, pp.170457-170473.
[12] Lee, K., Yeuk, H., Kim, J., Park, H. and Yim, K., 2016. An efficient key management solution for privacy masking, restoring and user authentication for video surveillance servers. Computer Standards & Interfaces, 44, pp.137-143.
[13] P. Buneman and W.-C. Tan, "Provenance in Databases," Proc. ACM SIGMOD, pp. 1171- 1173, 2018.
[14] Y. Cui and J. Widom, "Lineage Tracing for General Data Warehouse Transformations," The VLDB J., vol. 12, pp. 41-58, 2003.
[15] S.Czerwinski, R. Fromm, and T. Hodes, "Digital Music Distributionand Audio Watermarking," http://www.scientificcommons.org/43025658, 2017.
[16] Rahman, S.M.M., Hossain, M.A., Hassan, M.M., Alamri, A., Alghamdi, A. and Pathan, M., 2016. Secure privacy vault design for distributed multimedia surveillance system. Future Generation Computer Systems, 55, pp.344-352.
[17] Kim, J.S., Kim, M.G. and Pan, S.B., 2021. A study on implementation of real-time intelligent video surveillance system based on embedded module. EURASIP Journal on Image and Video Processing, 2021(1), pp.1-22.
[18] R. Agrawal and J. Kiernan, "Watermarking Relational Databases," Proc. 28th Int'lConf. Very Large Data Bases (VLDB '02), VLDB Endowment, pp. 155-166, 2019
[19] A. Jaiswal, V. Purohit, V. Jhawar, Y. Jadhav and K. Borhade, "Secure-e-Share: Data leakage Detection and Prevention with Secured Cloud Storage," 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2023, pp. 1-5, doi: 10.1109/SCEECS57921.2023.10063119.
[20] C. Li, Y. Huang, K. Kang, S. Dong and Y. Yao, "An Automatic Pipeline Leak Detection Robot Based on Compound Amphibious Motion," 2022 IEEE 2nd International Conference on Data Science and Computer Application (ICDSCA), Dalian, China, 2022, pp. 971-975, doi: 10.1109/ICDSCA56264.2022.9988574.
[21] D. Puthal, S. Nepal, R. Ranjan and J. Chen, "A Secure Big Data Stream Analytics Framework for Disaster Management on the Cloud," 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, NSW, Australia, 2016, pp. 1218-1225, doi: 10.1109/HPCC-SmartCity-DSS.2016.0170.
[22] A. Lay-Ekuakille, A. Trotta, G. Vendramin and P. Vanderbemdem, "FFT- based algorithm improvements for detecting leakage in pipelines," 2009 6th International Multi-Conference on Systems, Signals and Devices, Djerba, Tunisia, 2009, pp. 1-4, doi: 10.1109/SSD.2009.4956691.
[23] A. Awad, S. Kadry, G. Maddodi, S. Gill and B. Lee, "Data Leakage Detection Using System Call Provenance," 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS), Ostrava, Czech Republic, 2016, pp. 486-491, doi: 10.1109/INCoS.2016.95.
[24] Y. Canbay, M. Ulker and S. Sagiroglu, "Detection of mobile applications leaking sensitive data," 2017 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, Romania, 2017, pp. 1-5, doi: 10.1109/ISDFS.2017.7916515.
[25] S. Chhabra and A. K. Singh, "Dynamic data leakage detection model based approach for MapReduce computational security in cloud," 2016 Fifth International Conference on Eco-friendly Computing and Communication Systems (ICECCS), Bhopal, India, 2016, pp. 13-19, doi: 10.1109/Eco-friendly.2016.7893234.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY