Northern Economic Review
ISSN: 0262-0383
Vol. 16, No. 1 (2025)
DOI: https://doie.org/10.10399/NER.2025878770

Controlling and Protecting User-Sensitive Data Breaches Using a Secure Computing-on-Demand Service Network System

[1] D.Saravanan, [2] Dr. Dennis Joseph, [3] Dr. Maruthy Subramanyam, [4] W Wuriti Kavya
[5] Vindhya Pati

[1,2,3] Faculty of Operations & IT, ICFAI Business School (IBS), Hyderabad,
The ICFAI Foundation for Higher Education (IFHE)
(Deemed to be university u/s 3 of the UGC Act 1956)
Hyderabad-India.
[4] Project Developer, Intrinsic Global Communications Pvt Ltd, Hyderabad, Telangana, India.

Abstract: Data breaches are one of the most significant threats to the user community, especially as individuals increasingly adopt digital platforms. Today, most user operations rely heavily on the internet and smart gadgets. Moveable receivers, in particular, have become important for carrying out everyday activities. Various applications, including those for education, business, payments, and more, depend on network connectivity. However, this growing reliance on digital platforms also increases the risk of data theft and breaches. As users engage with different applications, their sensitive data is collected and either stored locally on their devices or on network servers. This creates potential vulnerabilities, putting their information at risk. In this proposed work, we address these security concerns by introducing a computing-on-demand service for data storage. Instead of storing sensitive information on local devices, the data is securely stored on demand in a distributed environment. This technique aims to enhance security by reducing the risk of local device breaches. The experimental setup and results demonstrate that the proposed approach significantly improves data security and effectively reduces the occurrence of security breaches, providing better protection for users' sensitive information.

Key terms: Data Breaches, Data security, mobile connection, Computing on Demand on service, Data vulnerable.

1. Introduction

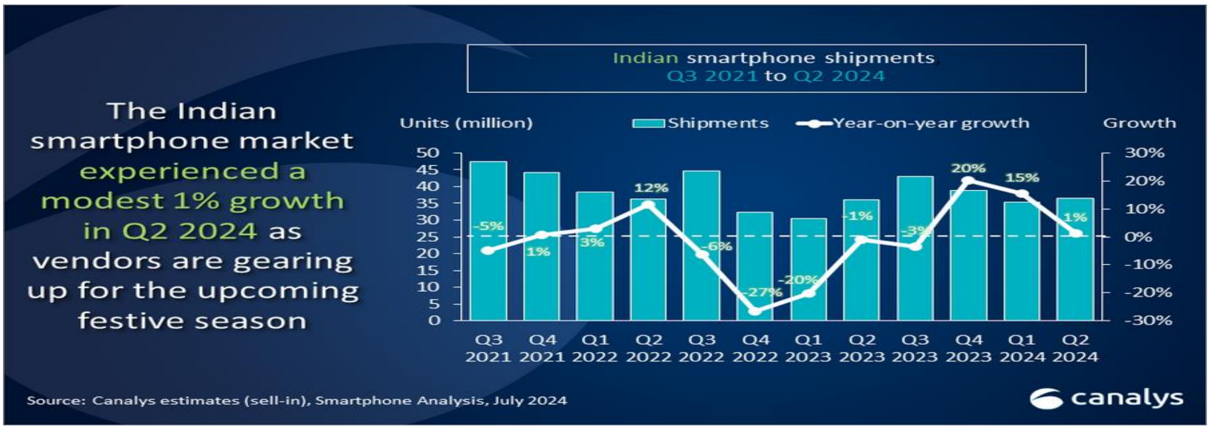
The use of smart gadgets is increasing every year, and this growth is accelerating by the second due to various factors. Today, users rely on these devices not only for entertainment but also for education, payments, communication, booking, information retrieval, and more. As the usage of gadgets continues to rise, data storage and management have become major challenges for many users[1]. To keep up with the growing demand, users frequently purchase higher-capacity storage devices. This trend continues year after year, as shown in Figures 1 and 2, which illustrate the increasing adoption of smartphones and the rise in storage capacity. The need for more storage is driven by the large number of applications users install on their devices within just a few days of purchasing them.

However, this widespread usage introduces significant security threats. Each time a user installs and interacts with an application, the service provider collects sensitive information, often before the user even begins using the service. This data is then stored either on the user’s device or on the company’s network. Even if the user later uninstalls the application, the credentials collected during the initial usage often persist in the provider's system. This practice makes smartphones highly vulnerable to data breaches. To mitigate this risk, the proposed work introduces a computing-on-demand storage mechanism. Instead of storing sensitive information on local devices or with third-party service providers, the data is securely stored in a centralized, high-security environment. This ensures that only authorized users can access the information.

1.1 The proposed approach offers several advantages:

- Enhanced Security: Storing data in a secure, centralized location reduces the risk of unauthorized access or data leakage from multiple storage points.
- Data Privacy: Even if users uninstall an application, their credentials and sensitive data remain protected in the centralized storage.
- Cost Efficiency: While the centralized storage solution may involve some additional costs, it is a worthwhile investment compared to the potential risks and damages caused by data breaches.

The growing affordability of smart gadgets has made them accessible to a larger population. However, most handlers are unacquainted of where their thoughtful evidence is stored. Many do not read the terms and conditions when installing applications, making them more vulnerable to data collection and breaches. Furthermore, users often share their credentials without hesitation, which makes them easy targets for hackers and data exploiters. This paper presents a mechanism for securely collecting and handling sensitive user data. The experimental study demonstrates that the proposed computing-on-demand system significantly reduces data breaches compared to the current storage methods, offering a more secure and reliable alternative for managing sensitive information.



Source: Canalys estimates (sell-in), Smartphone Analysis, July 2024

Fig 1. Smart phone users in India[2]

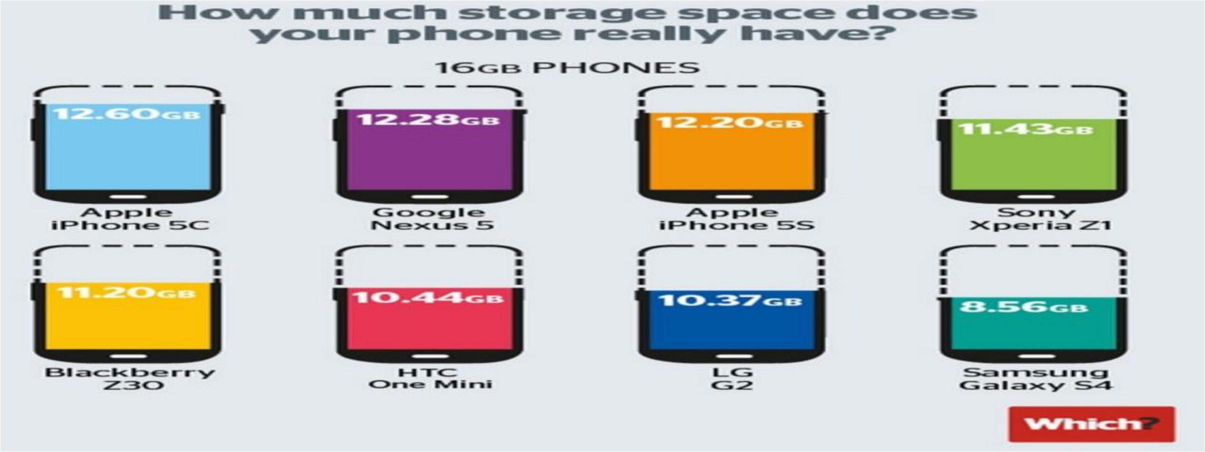
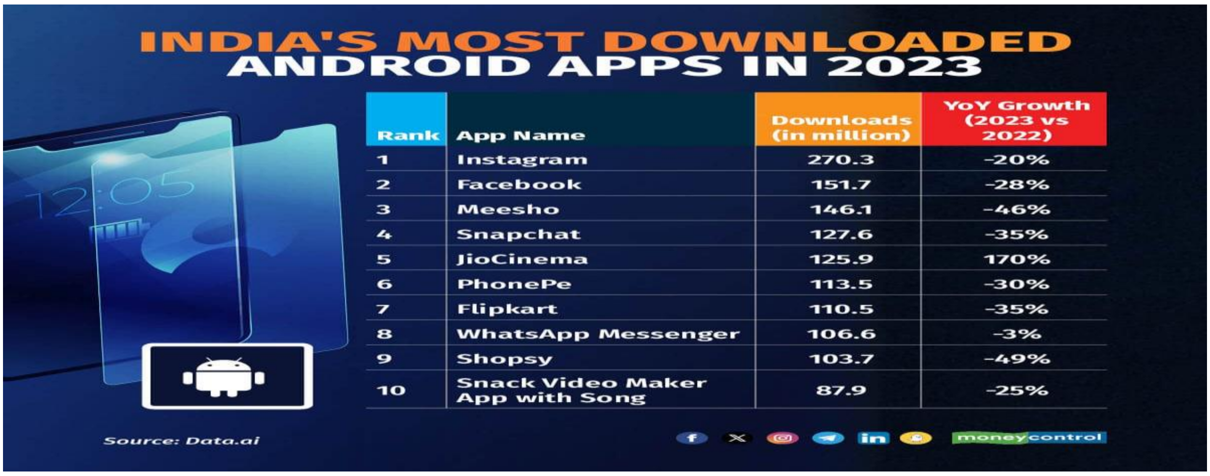


Fig 2 –Smart phone storage[3]

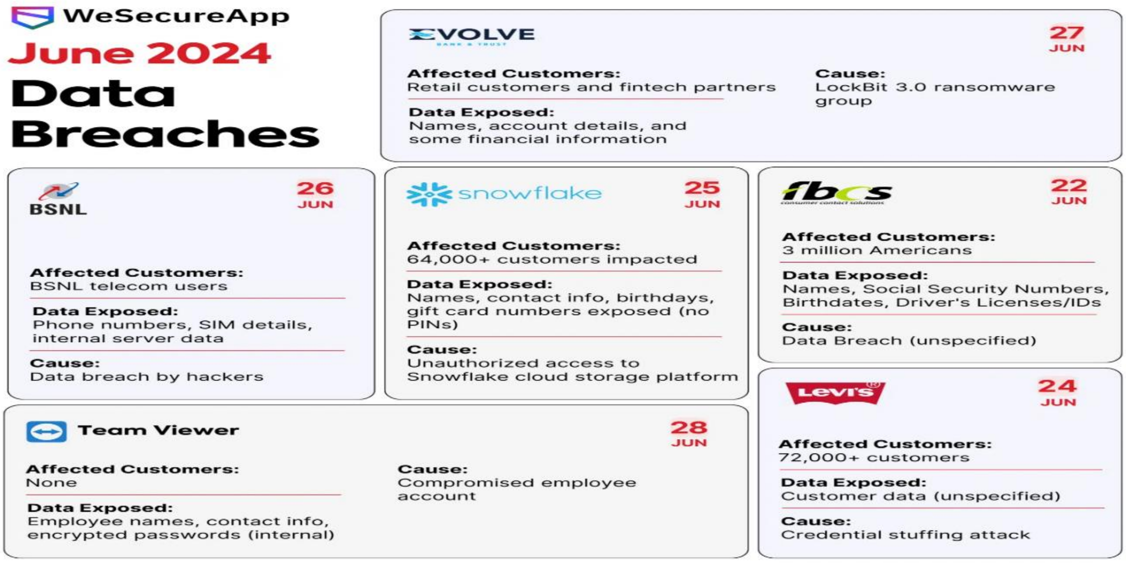

INDIA'S MOST DOWNLOADED ANDROID APPS IN 2023

Rank	App Name	Downloads (in million)	YoY Growth (2023 vs 2022)
1	Instagram	270.3	-20%
2	Facebook	151.7	-28%
3	Meesho	146.1	-46%
4	Snapchat	127.6	-35%
5	JioCinema	125.9	170%
6	PhonePe	113.5	-30%
7	Flipkart	110.5	-35%
8	WhatsApp Messenger	106.6	-3%
9	Shopsy	103.7	-49%
10	Snack Video Maker App with Song	87.9	-25%

Source: Data.ai

moneycontrol

Fig 3-Number of Apps installed on the device[4]


WeSecureApp

June 2024 Data Breaches

EVOLVE BANK & TRUST
27 JUN
Affected Customers: Retail customers and fintech partners
Data Exposed: Names, account details, and some financial information
Cause: LockBit 3.0 ransomware group

BSNL
26 JUN
Affected Customers: BSNL telecom users
Data Exposed: Phone numbers, SIM details, internal server data
Cause: Data breach by hackers

snowflake
25 JUN
Affected Customers: 64,000+ customers impacted
Data Exposed: Names, contact info, birthdays, gift card numbers exposed (no PINs)
Cause: Unauthorized access to Snowflake cloud storage platform

fbcs consumer contact solutions
22 JUN
Affected Customers: 3 million Americans
Data Exposed: Names, Social Security Numbers, Birthdates, Driver's Licenses/IDs
Cause: Data Breach (unspecified)

Team Viewer
28 JUN
Affected Customers: None
Data Exposed: Employee names, contact info, encrypted passwords (internal)
Cause: Compromised employee account

Levi's
24 JUN
Affected Customers: 72,000+ customers
Data Exposed: Customer data (unspecified)
Cause: Credential stuffing attack

Fig 4 Data breach in june 2024(Source: https://wesecureapp.com/wp-content/uploads/2024/07/June-Data-Breaches-2024-1536x1536.png.webp).

2.Problem Analysis

The proposed system addresses the issues present in existing methodologies by highlighting how collected data needs to be protected and how it is often easily leaked—either by service providers or due to user negligence.[5] This work also examines the advantages and disadvantages of the proposed system. In this study, we discuss how the new approach improves upon the current system by enhancing performance and storage efficiency. Furthermore, the paper explores how the proposed system differs from existing solutions, not only in terms of methodology but also in its overall functionality. To introduce a new technology, it is essential to first identify the drawbacks of the current system and understand how the proposed solution offers operational improvements. This analysis helps demonstrate how the new system effectively addresses the limitations of the existing technology, making it a more secure and reliable alternative.

3.Surviving arrangement

The existing mechanism collects users' sensitive data either knowingly or unknowingly. After purchasing a smart device, most users install various applications for their day-to-day activities[6]. These apps continuously collect and store information, even if the user stops using them. The collected data often persists somewhere on the network, even after the app is uninstalled, which increases the risk of data breaches and compromises user security. In addition to data storage, smart devices also track and store users' search patterns. Every time users search for specific functions or services, this information is recorded either on the local device or somewhere in the network. This ongoing collection and storage of sensitive information make users increasingly vulnerable to data exploitation and privacy risks.

3.1Drawback of Surviving arrangement

1. Lack of Security: The existing system offers minimal protection for users' sensitive data.
2. Frequent Data Breaches: Data breaches occur easily due to insufficient security measures.
3. Lack of Transparency: Users have no clear information about where their credentials are stored.
4. Mandatory Data Sharing: Applications often require users to share sensitive data to function properly.
5. Forced Information Disclosure: Sharing personal information is often mandatory, leaving users with no choice.
6. Limited Privacy: Many applications compromise user privacy by collecting and storing excessive data.

|4. Overcome of prospective mechanism

In this proposed work, we address these security concerns by introducing a computing-on-demand service for data storage. Instead of storing sensitive information on local devices, the data is securely stored on demand in a distributed environment. This technique aims to enhance security by reducing the risk of local device breaches [7]. The experimental setup and results demonstrate that the proposed approach significantly improves data security and effectively reduces the occurrence of security breaches, providing better protection for users' sensitive information.

4.1Advantage of the prospective mechanism

1. No Local Data Storage: User data is not stored on local devices, reducing the risk of unauthorized access.
2. Centralized Storage with Enhanced Security: Data is kept in a single, highly secure central storage, increasing overall security.
3. Simplified Tracking: Storing information in a single location makes tracking and managing data easier.
4. Elimination of Data Breaches: Centralized and secure storage significantly reduces the likelihood of data breaches.
5. On-Demand Data Storage: Information is stored using a computing-on-demand mechanism, improving the efficiency of data retrieval.
6. More Accurate and Relevant Results: The improved storage and search process provides users with more precise and relevant information.
7. Enhanced Privacy Protection: Centralized storage ensures better privacy and protection of sensitive information.

5.Prospective mechanism

In the proposed mechanism, illustrated in the figure above, the process begins with the administrator, who generates and manages the users participating in the system. Each user's credentials are collected, validated, and stored in the database. To ensure privacy and security, the data is converted into an unreadable format and stored on the computing-on-demand network [8]. All user information is kept in a single, centralized repository managed by a dedicated administrator. This ensures that sensitive data is highly protected and not scattered across multiple locations. When users want to access additional applications, their credentials are automatically shared through this centralized system. As a result, users do not need to repeatedly provide their personal information to third-party service providers.

Even when users submit a query to retrieve specific information, the network verifies their identity and finds the nearest relevant solution. The information is then shared only with the registered user. This entire setup is designed exclusively for authenticated users, ensuring that their data is never directly exposed to external service providers. The network administrator handles all credential management and data sharing securely. To maintain high security, each time a user makes a request, a unique private key is generated and shared between the user and the service administrator [9]. This key is used for authentication, and only after successful validation is the user granted access to the requested information. This mechanism ensures secure and controlled access to data.

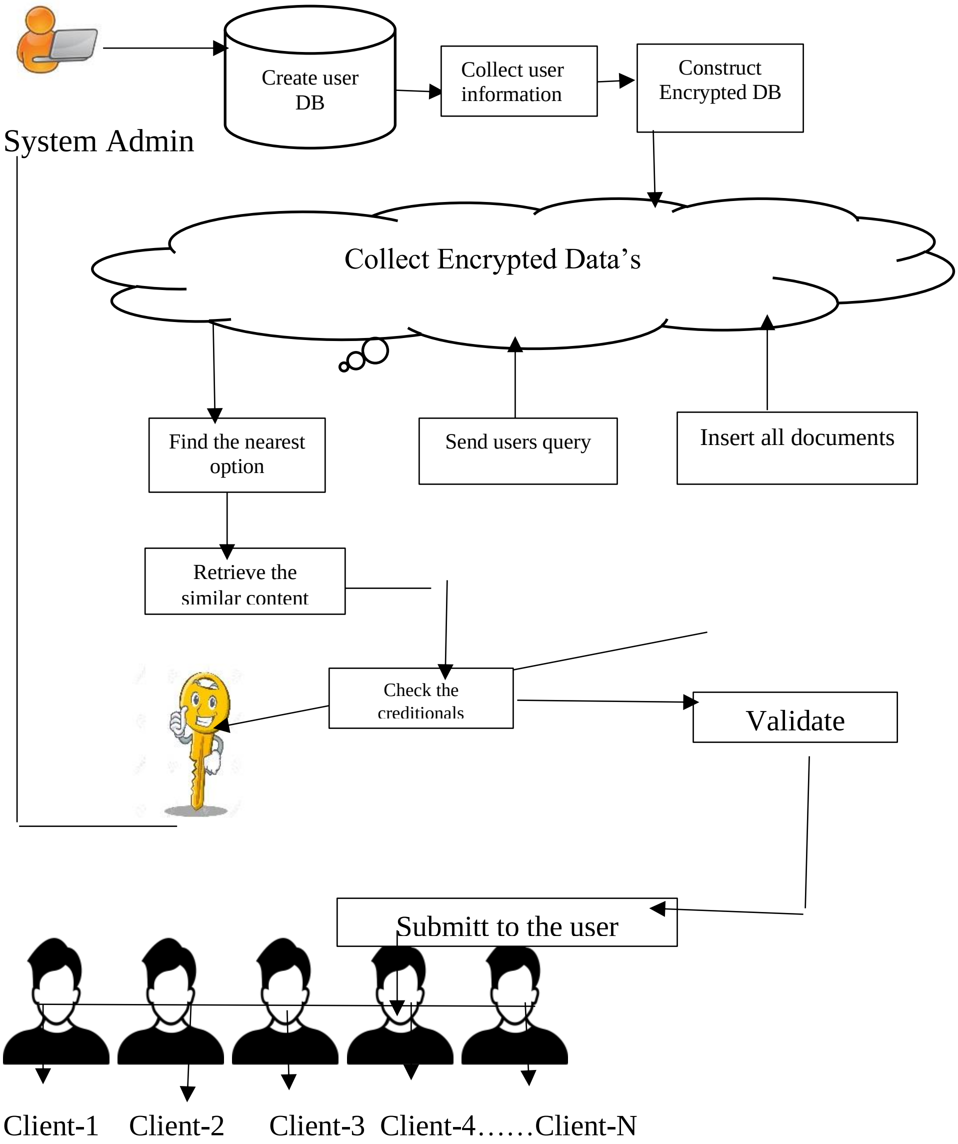


Fig 5. Prospective mechanism

5.1 The proposed system offers several advantages over traditional mechanisms:

- One-Time Registration: Users only need to register once. After registration, their information is securely stored and is never shared externally.
- Enhanced Privacy: All user credentials are encrypted and stored in a single, highly secure repository, significantly improving privacy protection.
- Authentication-Based Access: Even registered users must undergo authentication before accessing any information, ensuring that only authorized individuals can retrieve data.
- No Local Data Storage: Unlike traditional systems, no user information is stored on local devices (e.g., smartphones or local networks). All data is stored on the on-demand service provider's network, enhancing security and minimizing risks.
- Efficient Query Processing: With data centrally stored, query execution is faster and more efficient, improving overall system performance.

- Stronger Data Protection: Since the entire process is managed by a central administrator and involves encryption and authentication, the system effectively prevents data breaches.

The experimental results demonstrate that the proposed technique significantly enhances user privacy and security compared to existing methods. By eliminating local storage and using a centralized, encrypted repository, the system prevents data leaks and ensures efficient, secure, and reliable data processing.

6. Prospective mechanism functions

6.1 Create and collect users creational.
6.2 Create user Database with encrypted data's
6.3 Stored on compute on Demand service
6.4 Find the nearest service operations.
6.5 Retrieve and return to the user.

6.1 Create and collect users creational

The first and fundamental operation of the process is to collect and store users' details. This process gathers all the necessary credentials of the users and securely stores them. It is also referred to as the user registration process, as the proposed system can only be accessed by registered users. One of the main drawbacks of the existing system is that whenever a user attempts to access a new application or make a query from the network, their credentials are repeatedly collected by the service provider[10]. Users often have no knowledge of where this information is stored. In most cases today, when users visit specific websites, certain details are automatically filled in—sometimes knowingly and sometimes unknowingly. This practice can lead to issues, as sensitive information such as credit card details, bank names, card expiry dates, and, in rare cases, authentication tokens are collected and stored. This increases the risk of credential exposure and misuse by unauthorized individuals.

To mitigate this issue, the proposed system collects the user's credentials only once during the initial registration. These credentials are stored on a single, secure site. An added advantage of this method is that the stored user information is converted into an unreadable format , ensuring that even authorized users cannot directly read the data. Another benefit of the proposed system is that, during the initial stage, the user's information is collected, encrypted, and stored on a compute-on-demand service. This ensures that the information is not saved on the user's local system or any local network, but only on an authorized network. With each access attempt, the system verifies the user's credentials, and only upon a successful match are the details extracted and shared securely[11].

The primary advantage of the proposed system is that user credentials are collected only once—during the initial registration and only after proper authentication. Subsequently, whenever the user logs in or accesses any application, their credentials are securely retrieved and shared with the respective service providers through an authenticated channel. Since the credentials are not stored elsewhere, this method significantly enhances efficiency and security. This process is shown in the below figure.

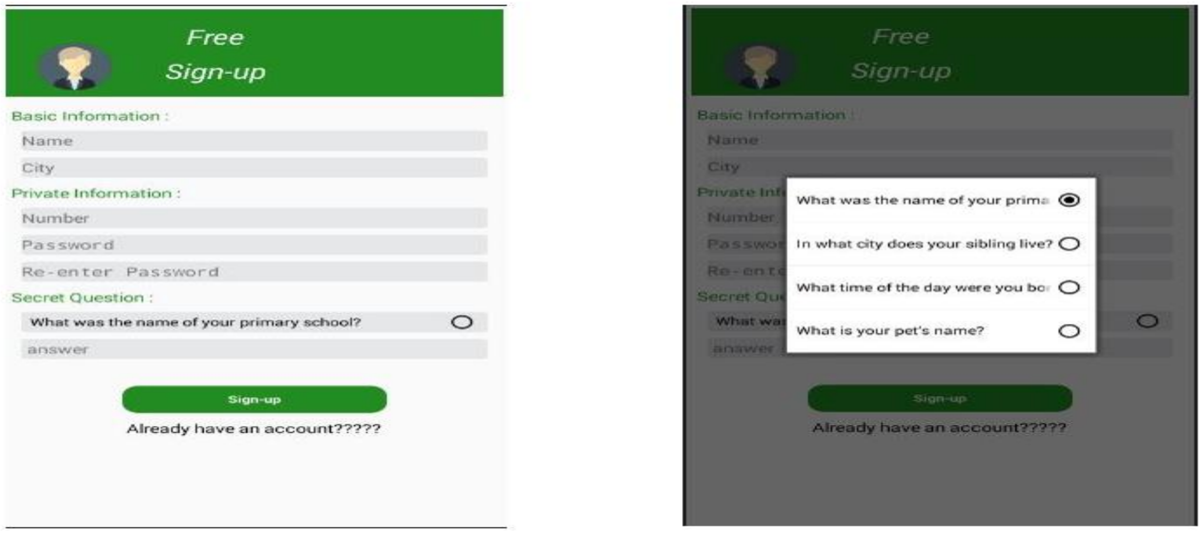
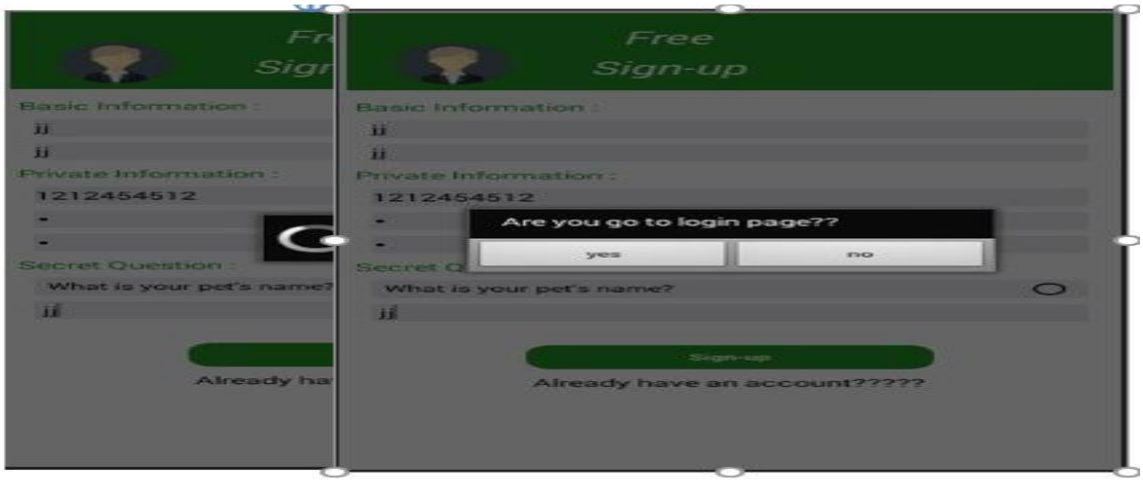

Free
Sign-up
Basic Information :
Name
City
Private Information :
Number
Password
Re-enter Password
Secret Question :
What was the name of your primary school? ○
answer
Sign-up
Already have an account?????
What was the name of your prima ●
In what city does your sibling live? ○
What time of the day were you bo ○
What is your pet's name? ○

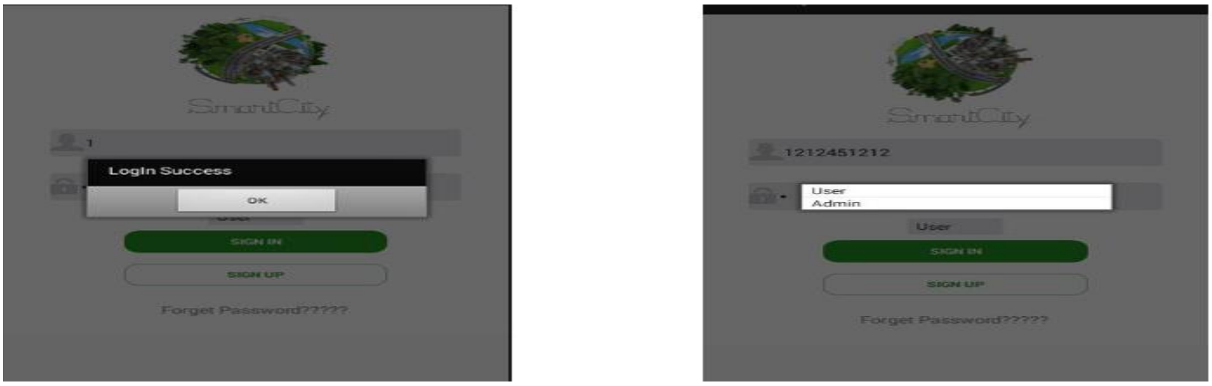
Fig 6. Create and collect users creational form.



jj
jj
1212454512
What is your pet's name?
jj

Are you go to login page??

Fig 7. User creditionals created successfully



1

Login Success

1212451212

Fig 8. User login creditionals creations.

6.2 Create user Database with encrypted data's:

Each time a user installs and interacts with an application, the service provider collects sensitive information, often before the user even begins using the service. This data is then stored either on the user's device or on the company's network. Even if the user later uninstalls the application, the credentials collected during the initial usage often persist in the provider's system [12]. An added advantage of the proposed system is that the stored user information is converted into an unreadable format ensuring that even authorized users cannot directly read the data. Another benefit is that, during the initial stage, the user's information is collected, encrypted, and stored on a compute-on-demand service. This ensures that the information is not saved on the user's local system or any local network, but only on an authorized network. With each access attempt, the system verifies the user's credentials, and only upon a successful match are the details extracted and shared securely. Smartphones are particularly vulnerable to data breaches due to the widespread storage of sensitive information on local devices. To mitigate this risk, the proposed system introduces a computing-on-demand storage mechanism. Instead of storing sensitive information on local devices or with third-party service providers, the data is securely stored in a centralized, high-security environment. This ensures that only authorized users can access the information, significantly enhancing data privacy and security.

6.3 Stored on compute on Demand service

The main drawback of the existing system is that each time a user wants to access information from the network or download and use a service provider's application, they are required to enter their sensitive credentials. Users have no clear knowledge of where this information is stored or whether it is shared with third parties. In many cases, users are forced to share personal information just to access the desired content [13]. Most internet users prioritize using the application over safeguarding their credentials. For example, when a user wants to play an online game or access a service, they are often required to provide details such as their name, date of birth, and basic account information. Each time users download a new application, they must repeatedly share the same sensitive information. This practice creates significant privacy risks, as users are unaware of where their credentials are stored or how they are used.

6.3.1 To overcome these drawbacks, the proposed system introduces a centralized and highly secure mechanism:

6.3.1.1 User Registration on a Trusted Site:

- First, the user creates an account on a trusted site, where their information is collected and stored in encrypted format.
- This encryption ensures that the data is protected and cannot be accessed by unauthorized service providers.

6.3.1.2 Improved Security through Compute-on-Demand Storage

- The encrypted information is not stored on the user's local device or any local network.
- Instead, it is securely stored on a compute-on-demand service, where only a pool of authorized users has access.
- This ensures that all user information is centralized on a single, highly secure site.

6.3.1.3 Controlled Data Sharing

- When a service provider needs the user's information, it is shared only through a proper authentication mechanism.
- Each time a service request is made, the user’s credentials are verified by the system.
- Only if the request is valid and properly authenticated are the credentials shared; otherwise, the request is denied.

6.3.1.4 Triple-Layer Protection Against Hacking Attempts:

- The compute-on-demand service stores all user information in an encrypted format.
- Even if hackers attempt to steal the data, they cannot read the information without the encryption key.
- This ensures triple-layer protection for user information, maintaining a highly secure environment.

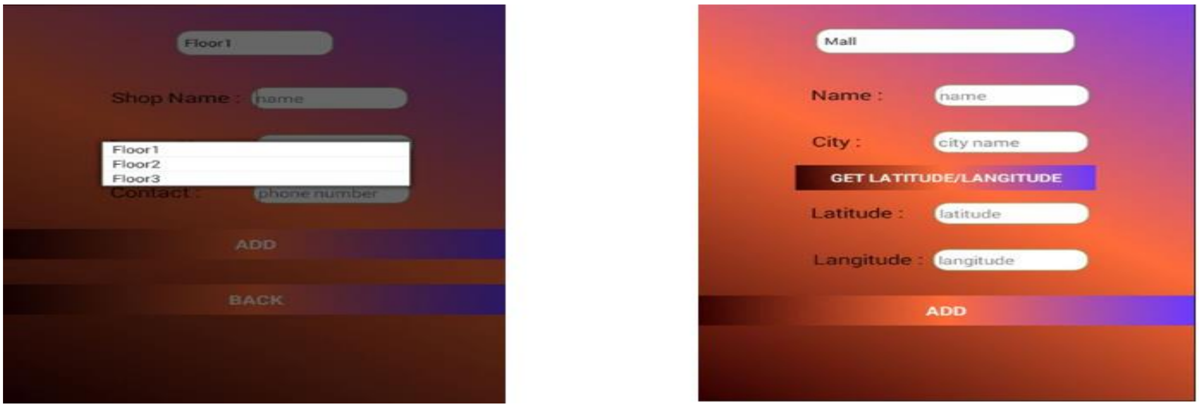
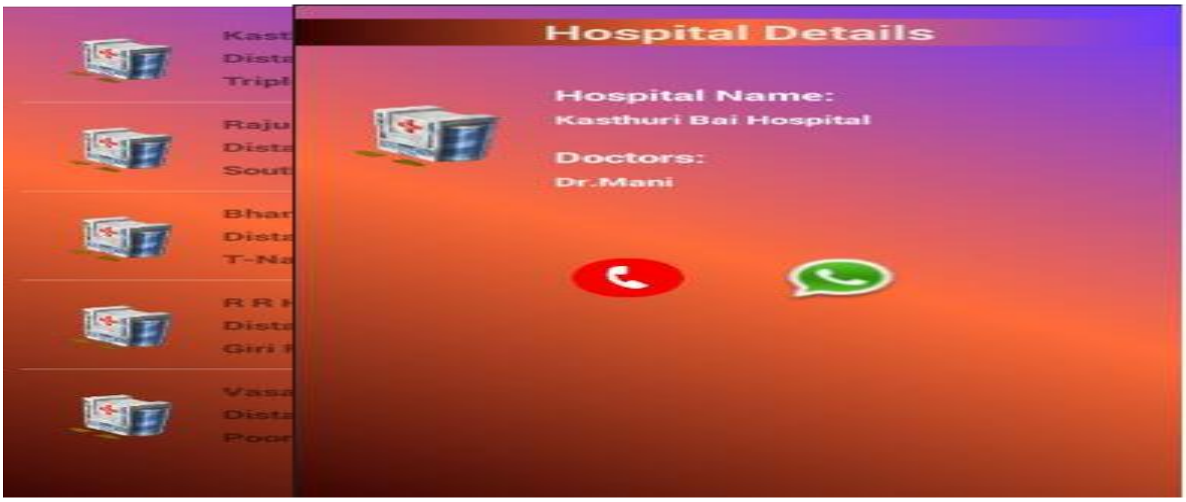


Fig 9. user’s details are collected and stored.



Hospital Details

Hospital Name:
Kasthuri Bai Hospital

Doctors:
Dr.Mani

Fig 10. created details stored on computing on demand service provider.

6.4 Find the nearest service operations

An added advantage of the proposed system is that the stored user information is converted into an unreadable format, ensuring that even authorized users cannot directly read the data. Another benefit is that, during the initial stage, the user's information is collected, encrypted, and stored on a compute-on-demand service[14]. This ensures that the information is not saved on the user's local system or any local network, but only on an authorized network. With each access attempt, the system verifies the user's credentials, and only upon a successful match are the details extracted and shared securely.

Additionally, each time the system receives a service request, it not only verifies the credentials but also identifies the nearest location to fulfil the user's request. Since all necessary information is collected and stored on the compute-on-demand system, any service provider that needs the user's credentials can access the nearest available data[15]. This reduces latency and ensures that the required information is immediately shared with the user. To achieve this, the system registers the user's credentials along with their most frequently used applications. This information is securely stored by the compute-on-demand service provider. Upon receiving a request, the system efficiently retrieves and shares the information in real time, enhancing both speed and performance.

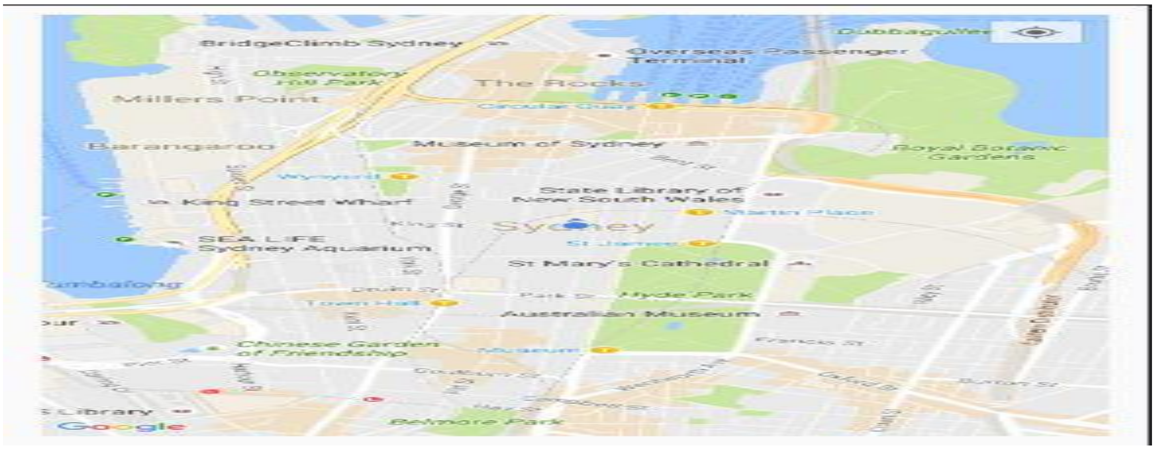


Fig 11. creating nearest point information’s.

6.5 Retrieve and return to the user

However, this widespread usage introduces significant security threats. Each time a user installs and interacts with an application, the service provider collects sensitive information, often before the user even begins using the service. This entire setup is designed exclusively for authenticated users, ensuring that their data is never directly exposed to external service providers[16]. The network administrator handles all credential management and data sharing securely. To maintain high security, each time a user makes a request, a unique private key is generated and shared between the user and the service administrator. This key is used for authentication, and only after successful validation is the user granted access to the requested information. This mechanism ensures secure and controlled access to data.

7.Conclusion and future enhancement

Today, most user operations rely heavily on the internet and smart gadgets. Mobile phones, in particular, have become essential for carrying out everyday activities. Various applications, including those for education, business, payments, and more, depend on network connectivity. Many do not read the terms and conditions when installing applications, making them more vulnerable to data collection and breaches. Furthermore, users often share their credentials without hesitation, which makes them easy targets for hackers and data exploiters. This paper presents a mechanism for securely collecting and handling sensitive user data. To mitigate this risk, the proposed system introduces a computing-on-demand storage mechanism. Instead of storing sensitive information on local devices or with third-party service providers, the data is securely stored in a centralized, high-security environment. This ensures that only authorized users can access the information, significantly enhancing data privacy and security.

8.References:

1. Schneider. (2014). Go green in the city Available: http:// 2014.gogreeninthecity.com/smart-cities.html.
2. Source https://www.canalys.com/newsroom/india-smartphone-shipments-Q2-2024)
3. Source: https://www.zdnet.com/article/how-much-free-storage-space-does-your-smartphone-really-have/)
4. Source: https://images.moneycontrol.com/static-mcnews/2024/01/Indias-app-economy-2024_001.jpg)
5. M. Egele, C. Kruegel, E. Kirda, and G. Vigna, “PiOS: Detecting privacy leaks in iOS applications,” in Proc. 18th Annu. Netw. Distrib. Syst. Security Symp., 2011, pp. 1–15.
6. W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, “Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones,” in Proc. USENIX 9th Conf. Oper. Syst. Design Implementation, 2010, pp. 1–6.
7. Manaskumar ,S.Senthil Kumar ,D.Saravanan, “SQL Injection monitoring security vulnerabilities in web applications” ,International Journal of Information Technology (IIJIT), Volume -02, Issue -03, March 2014, Pages 01-06, ISSN : 2321-5916.
8. D Saravanan, Dr. Dennis Joseph,”An Enhanced Three Factor validation arrangement with Biometric Privacy safety Using Finger print”, In the proceeding of international Conference on Emerging Technologies, Analytics and Operations (ICETO-2025) Page 66, March 07-08, 2025
9. W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri, “A study of Android application security,” in Proc. 20th USENIX Conf. Security, 2011, p. 21.
10. A. Bose, X. Hu, K. G. Shin, and T. Park, “Behavioral detection of malware on mobile handsets,” in Proc. ACM 6th Int. Conf. Mobile Syst., Appl., Services, 2008, pp. 225–238.
11. A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, “A survey of mobile malware in the wild,” in Proc. ACM 1st Workshop Security Privacy Smartphones Mobile Devices, 2011, pp. 3–14.
12. S. Vaithyasubramanian, A. Christy, D.Saravanan, “An Analysis of Markov Password Against Brute Force Attack for Effective Web Applications”,Applied Mathematical Sciences, Vol. 8, September 2014, no. 117, 5823– 5830, ISSN 1312-885X. (IF 0.781)
13. J. Cheng, S. H. Wong, H. Yang, and S. Lu, “Smartsiren: Virus detection and alert for smartphones,” in Proc. ACM 5th Int. Conf. Mobile Syst., Appl. Services, 2007, pp. 258–271.

14. S.Vaithyasubramnian, A.Christy, D.Saravanan, “Two factor authentication for secured login in support of effective information preservation and network security” ARPN Journal of Engineering and Applied Science, ISSN:1819-6608, Volume 10,No:05, March 2015, Pages 2053-2056.(IF 0.795)(
15. Appthority. (2014). App reputation report [Online]. Available: https://www.appthority.com/app-reputation-report/report/ AppReputationReportSummer14.pdf
16. L. Musthaler. (2013). At least 80% of mobile apps have security and privacy issues that put enterprises at risk [Online]. Available: http://www.networkworld.com/article/2163225/ infrastructure-management/at-least-80-of-mobile-apps-havesecurity- and-privacy-issues-that-put-ente.html