Solution for Securing Sensitive Data: Breach Prevention & Mitigation

Monika B , Sathvika Reena Kumari N and Dr.K SandhyaRani Kundra

[1] Gayatri Vidya Parishad College Of Engineering(A),Visakhapatnam, India
Dept.Information Technology
monikabattula28@gmail.com

[2] Gayatri Vidya Parishad College Of Engineering(A),Visakhapatnam, India
Dept.Information Technology
sathvikareena7@gmail.com

[3] Gayatri Vidya Parishad College Of Engineering(A),Visakhapatnam, India
Associate Professor,Dept. Of Information technology
sandhyaranikk@gvpce.ac.in

Abstract. Data breaches of any nature strike industries with various adverse outcomes, both tangible returns and reputation loss that in future erodes the public trust. Given that such operational environments are data centric in nature, it is now more than ever essential to be able to protect sensitive data and still be able to maintain the confidence of the public. The BaaS model that supports data remotely further complicates issues of data privacy such as protecting the data from unauthorized access or untrusted third party service providers. The authors of this article seek and respond to these issues offering methods of performing SQL querying on encrypted data thereby reducing the amount of data that will need to be decrypted at the client's end. The paper also suggests improving contemporary practices with rapidly developing prevention approaches, effective management and public information about users and potentially impacted populations in case of the data protection breach. The paper also addresses a number of recent historical cases of data breaches, an overview of the modern preventive tools and practices for data leakages, and new challenges that occur in enterprise environments.

Keywords: Confidentiality Breach, Information Protection, Social Acceptance, Database as a Service, Secure Information, Structured Information Retrieval Commands, Organizational Security, Evaluation of Effects on Society.

1 Introduction

The Aadhaar information leak, a useful incident in Bharat's computerized documents, reveals single information for a large number of people, highlighting the vulnerability of biometric identification systems. The offence concerned illicit access to a large repository of unique facts, including names, trade, biometric data, and Aadhaar numbers, covering approximately 83 percent of the 2018 financial statements, an increase over the previous year. The scale of the breach trip terrors concerning self larceny (64%), economic fraud, and the decline in secrecy is unprecedented. The root cause of the lapse has been identified as the lack of proper defense measures (absence of coding mechanism, lax admission controls, and outdated security protocols), stressing the need for robust security protocols, comprehensive employee education, and tight entry controls.

The breach affected individuals and communities, including identity larceny (83% of transactions transgressed), fiscal fraud (83% of transactions transgressed), corrosion of confidentiality (75% of biometric data compromised), panics around the world due to surveillance and misuse, and a lack of faith in major institutions to protect individual facts. The data breach also had significant economic consequences, together with the average cost of data breaches worldwide of $ 3.92 million (we ourselves own the high cost of $ 8.19 million) and the estimated turnover of customers' employees reaching 3.9 % (up from 3.4 %) in 2018. Furthermore, affected consumers

commonly end their association with the organization, resulting in a loss of trade (customer compensation may remain able to recover, but companies still face the additional challenge of regaining confidence).
Moreover, the Aadhaar data breach has brought about serious security loopholes. To safeguard public figures, a number of vulnerability had existed close to outdated encryption methods, abuse of access control and vulnerability of protocols. The event grades have demanded a total overhaul of the security protocol especially in relation to the evolving subsequent coding techniques and strict sudden detours. Including fictional character, insider threat makes it necessary for stringent environmental verifications, increased employee training and awareness of cyber security as an impending measure against both insider and external threats. In the same way, this made even more incidences wherein financial statements had to be audited on regular basis because if systematic audit is not conducted frequently enough then holes may remain concealed indefinitely forever. The strong audit accounting model should be crafted before identifying and minimizing risks posed by those who are likely to be exploited through proper leadership ability while constant monitoring should always remain important.
The situation regarding the Aadhaar data left open a lot of motivations to attempt this possible answer to amplification of safety Oldies party without it being the system can also be explained through four points which include: 1. Proxy number storage for Aadhar card details 2. One-time proxy number generation with expiry date 3. Preventing third party data breach 4. Battle against forged aadhar cards

2 DPDP Laws and Issue of Parental Consent:

The Act specifies that individuals have the right to their records, can amend it or even demand deletion from storage systems which entail an unprecedented level of management control over data for any individual. One of its main aspects is getting an express consent from the owner prior to processing his/her data thereby, no information should be collected from respondents unless they were made aware about what type of information would be collected about them generally speaking ,and for what purpose(s). Additionally these consent forms must meet certain explicit requirements so that they can be followed appropriately.

The focus of this paper is on data localization; these certain types of personal data, which are particularly sensitive, must be stored in India so that their security can be enhanced and their laws can be implemented. As a result of this, the Indian Data Protection Board (IDPB) was established as a regulatory body to monitor compliance with these rules, resolve related disputes and levy penalties for violations. Organizations are obliged by law to report data breaches to the affected persons and also to DPBI without delay so that there is openness and quick action can be taken to deal with the situation before it gets worse. For this reason, high levels of data protection are maintained in most organizations since it is also an encouragement for them due to stringent fines or penalties which come with non-compliance with its terms. Thus, all these provisions help ensure that individual's privacy is highly respected.

Also contained in this legislation are provisions for children's data protection, including a requirement for verifiable consent under section 9. Nevertheless, there are several problems associated with the implementation of these provisions especially concerning verification of age and what can be harmful to children. It appoints a data fiduciary which needs parental or guardian consent regarding collection of children data and prohibits illegal data processing or advertising/ micro-targeting toward children. Nonetheless, some organizations may not be obliged to do so as exemplified by health facilities and schools.
One of the key concerns has been how age restrictions that platforms must enforce are going to be implemented. This is very important because in many ways its framework provision is not clear hence making it hard, for instance, to observe the law. Also, there are other issues like withdrawal of parental consent or reaching legal adulthood in case of a child who must take precedence during this process.

The second one deals with storing biometric data in a technical way as well as problems which may arise trying to harmonize them into some protective measures defined by the Act. But mainly it still remains unspecified especially when it comes to consent between parents and their children and therefore increasing the difficulty to comply even further.

Several of these issues and their various possible solutions were discussed; still, all had some drawbacks. For instance, the very first discussed solution applying for the parent's DigiLocker app for consent using Aadhaar detail was set to be not feasible from the weaning and datum security perspective. Similarly, it wasn't easy to have an electronic token system that had the government's approval in practice. The latest proposal suggests that a graded approach, based on the level of risk involved, like AADC, is better, but even this may not smoothen the way for protection of children's data in the context of India.

All these issues thus give an idea about the complexity and the necessity of a properly constructed framework, along with a proper layout for the protection of children's data under DPDPA 2023, with regard to protection against data breach and compliance of various sectors.

3 Proposed Solution

3.1 The Proposed Architecture

The proxy number option for the purpose of securing Afar information can be dissected into three main stages, the importance of each in safeguarding Afar information and priming the system for any eventuality or hazard being critical:

1.Initialization & Proxy Assignment.
2.Proxy Number Management & Validity Check.
3. Data Breach Oversight & Response

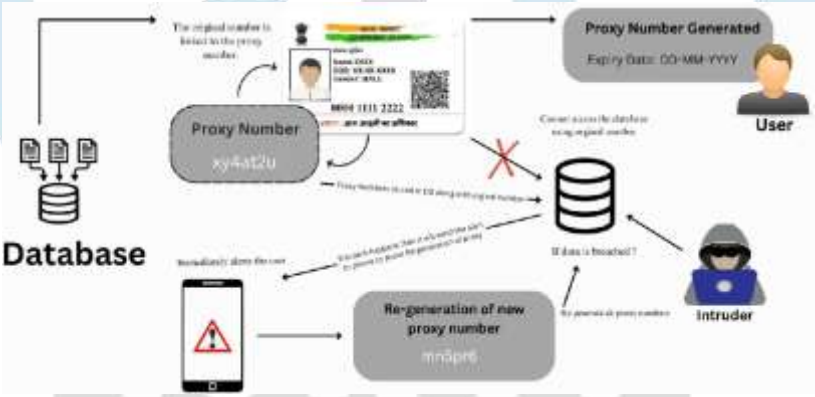

Fig. 1. Proposed Solution

Phase 1: Initialization & Proxy Assignment

1.Original Aadhaar Number Management:

The first step that the system takes is to have the actual Aadhaar number with it. This number is quite vital because the real identity of the user will be substituted by a proxy number so that true identity is hidden.

```
index.html > ...
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Number Validation</title>
</head>
<body>
    <h2>Enter Proxy Number Only !</h2>
    <form action="validate_proxy.php" method="POST">
        <input type="text" name="number" required>
        <button type="submit">Submit</button>
    </form>
</body>
</html>
```

Fig. 2. Index.html

2. Generate Proxy Number:

It creates a new proxy account number from the original Aadhaar number. It is called as 'attempted proxy' numbers and fits within a particular period of time.

3. User Registration:

In case of each new provider signup, this system would link any previously generated proxy numbers to subscribers. Unlike Aadhaar numbers, these temporary ones are used just for limited durations.

Phase 2: Proxy Number Management & Validity Check

1. Expiry Date Management:

With every normal operation of their system, they make sure to periodically verify whether a given proxy number is still valid or not including its date before it expires.

2. Proxy Number Validity Check:

- If the Proxy Number is Valid: The user experiences no changes in use, he/she should apply the proxy number.
- If the Proxy Number is Expired:In order for the user to posses a secure and valid proxy number remotely linked with his/her original Aadhaar number all the registrations through the system thereon generate a new one and alters its expiry date.

Phase 3: Data breach oversight & response.

1. Data Breach Scenario : The system is designed appropriately and know how they can work through when it comes to any data breach situations possible.

- If an Intruder Breaches the Original Aadhaar Number: In the worst-case or if no information is available, the system shows a message stating that the data is expired and thus ensures the user's anonymity and security of his personal data.
- If an Intruder Gains Access to the Proxy Number: They further illustrated that the prospect of data breach is recognized by the system and rebuffed by providing another proxy number.

Fig. 3. Validate_Proxy.php

- If the Expiry Date Approaches : Even when the breach occurs, the system will have pre-assign a new proxy number to reduce the effect and to continue with the security process.

3.2 Incident Response :

For instance, if the breach is detected or a proxy number is compromised, the system shall alert the citizens concerned through dissemination of the incident response plan.

Part of this plan will have guidelines on how they can safeguard their data and any other measures that they need to take to protect their Aadhaar details.

4 Experimental Setup and Results 4.1 Proxy Number

Usage

When the aforesaid proxy number is entered in the space provided, we can obtain details of the actual users from the ‘proxy_management. sql‘ database. This is because the original Aadhaar number is synched with the proxy number that makes it possible for the system to be relaying the user details as a result of the entered proxy number.

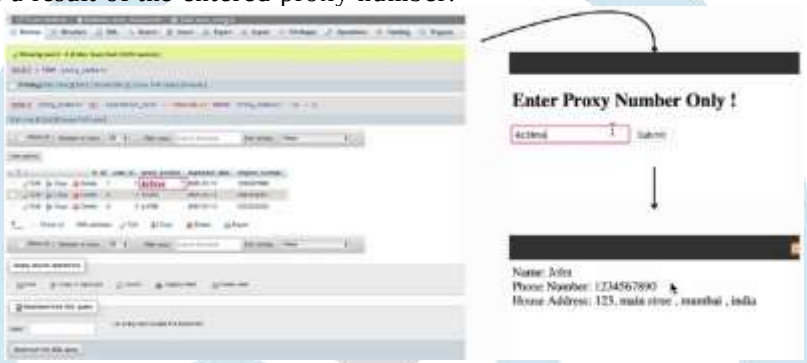

Fig. 4. User Details when Proxy number Entered

4.2 When using the Original Number

When we enter the original number in the given space, we cannot retrieve any information related to the user in the ‘proxy_management.sql‘ database. This means, according to the information in that database, it will not provide the user details and will simply return "not valid" or "expired."

Fig. 5. No Data found when original number Entered

4.3 When the Expiration Date of Proxy Number is Invalid

When the expiration date of the proxy number is invalid, the system will not retrieve the associated user information. Instead, it will indicate that the proxy number is either "expired" or "invalid," preventing access to any linked data. This ensures that only valid, non-expired proxy numbers can be used to access user details.

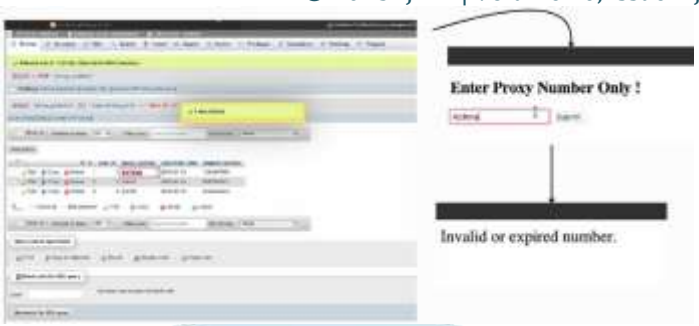

Fig. 6. When change in expiry date

5 Literature Review

The Aadhaar system plays a key role in India's digital identity setup, and people are talking a lot about how safe and private it is. Maulik (2024) found big weak spots in the Aadhaar system. He came up with a new method using three checks to stop unwanted access and data cheating. This work shows we need to make public data systems stronger to protect the Aadhaar database.

Thejaswini S (2022) had a similar idea. They suggested using blockchain and InterPlanetary File System (IPFS) together to keep Aadhaar details and fingerprints safe. This system makes sure people who should use citizen services can do so. It also double-checks for mistakes when making new Aadhaar cards.

The examination of the Aadhaar data breach by digiALERT (2024) brings to light the inadequacies in current security measures, highlighting insider threats and the absence of regular audits as significant contributors to the breach. The article calls for the implementation of robust encryption, stringent access controls, continuous monitoring, and increased public awareness to reinforce the cybersecurity infrastructure surrounding Aadhaar. Tech2 News Staff (2018) also looked into the Aadhaar data breach. They found

Reference	Key Contribution
Reshmi Maulik (2024)	Vulnerabilities of the Aadhaar system were identified by the authors and an algorithm has been proposed together with a three-factor authentication method to prevent unauthorized access and data fraud. This study particularly
Thejaswini S (2022)	A secure and authenticated system that intends to keep secured Aadhaar details and fingerprints by using blockchain and IPFS was suggested by the authors in such a way that only authenticated users can have access to citizen
digitALERT (2024)	The paper talks about how Aadhaar data got leaked in India. It points out that poor security, insider threats, and not enough audits led to this. The paper stresses the need for
Tech2 News Staff (2018)	The system needs new encryption methods because the old ones failed after a breach. This breach exposed many users' data, including their fingerprints. This makes identity theft or online money scams more likely. It shows we need tough

Table 1. Summary of Key Contributions on Aadhaar System Security

major security problems like old encryption and weak access controls. These issues have caused big risks, including identity theft and money fraud. This study shows we need better cybersecurity plans to keep the sensitive data in the Aadhaar system safe.

Acknowledgments. We want to thank Dr. I.V.S.Venugopal(B.Tech. M.Tech.,Ph.D) Assistant Professor and Dr K SandhyaRani Kundra Associate Professor Department of Computer science and Infomation Technology for helping and giving ideas to implement the algorithm .

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

5.1 **Conclusion and Future Scope**

The suggested proxy number setup offers a full fix to boost Aadhaar safety by tackling key weak spots in the system. It uses a step-by-step plan of setup, proxy handling, and leak response to protect users' identities and private data. Proxy numbers that expire add another shield keeping original Aadhaar info safe even if there's a breach.

On top of that, using blockchain and IPFS tech makes data storage more secure letting approved users get access. This method cuts down on the chances of unwanted access and data cheating making the Aadhaar system safer and more trustworthy overall.

References

1. Shaurya Shekhar, Vasantha W B , and Aarushi Thakral, "Privacy and Security in Aadhaar," Student. Professor. VIT University, Vellore, Tamil Nadu, India, vol. 6,Iss. 4, pp. 2321-9939, IJEDR 2018.
2. Zhang, X.,Yadollahi, M.M., Dadkhah, S., Isah, H., Le, D-P. and Ghorbani, A.A.(2022)'Data breach: analysis, countermeasures and challenges', Int. J. Information and Computer Security, Vol. 19, Nos. 3/4, pp.402–442.
3. Ogbuke, N.J.; Yusuf, Y.Y.; Dharma, K.; Mercangoz, B.A. Big data supply chain analytics: Ethical, privacy and security challenges posed to business, industries and society. Prod. Plan. Control. 2022, 33, 123–137.
4. Foerderer, J.; Schuetz, S.W. Data breach announcements and stock market reactions: A matter of timing? Manag. Sci. 2022, 68, 7298–7322.
5. Farsi, M.; Ali, M.; Shah, R.A.; Wagan, A.A.; Kharabsheh, R. Cloud computing and data security threats taxonomy: A review. J. Intell. Fuzzy Syst. 2020, 38, 2517–2527.
6. Alfawzan, N.; Christen, M.; Spitale, G.; Biller-Andorno, N. Privacy, data sharing, and data security policies of women's mhealth apps: Scoping review and content analysis. JMIR Mhealth Uhealth 2022, 10, e33735.
7. Gabriel Arquelau Pimenta Rodrigues, André Luiz Marques Serrano, Amanda Nunes Lopes Espiñeira LemosData 2024, 9(2), 27; https://doi.org/10.3390/data9020027.
8. Ong, E.I. Singapore report: Data protection in the Internet. In Data Protection in the Internet; Springer: Cham, Switzerland, 2020; pp. 309–347.
9. Shires, J. The Simulation of Scandal: Hack-and-Leak Operations, the Gulf States, and US Politics (Fall 2020). Tex. Natl. Secur. Rev. 2020, 3, 10–29.
10. Mantelero, A. The future of data protection: Gold standard vs. global standard. Comput. Law Secur. Rev. 2021, 40, 105500.