e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:01/January-2021 Impact Factor- 5.354 www.irjmets.com

SURVEY ON COLLEGE APPLICATION DEVELOPMENT AND DATABASE AS A SERVICE (DBaaS)

Siddharth Koul[*1], Rayan Rouf[*2], Sarthak Madaan[*3], Suman M[*4]

[*1,2,3]Student, Department of Computer Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India.

[*4]Assistant Professor, Department of Computer Science and Engineering, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India.

ABSTRACT

In the present world, many colleges are developing applications for its students and faculty on various platforms such as web based, android and so on. Some of these applications require user data. This data is then stored in various types of databases. These databases can be company owned or being provided by a database service provider. A part or whole of the data provided by the user can be critical and databases are always prone to attacks for information. For this purpose, encryption is used to safeguard this data. This paper provides a survey of Database as a Service and security, applications developed for colleges and Firebase.

Keywords: Database as a Service, Firebase, security, encryption.

I. INTRODUCTION

The world has come a long way from storing all the data on a ledger to storing this data in a database. Colleges in past used to keep huge ledgers of data on students and faculty. Maintaining this data was a tiresome activity. The introduction of computers started a revolution in the education department. They started to host this data on their servers. Now, maintaining data became easier as it was easier to keep track of activities using computer and operations became much more efficient as insertion, modification and deletion of data could be done without creating any mess. With time, applications were built to facilitate students and faculty with the feature of interacting with each other and also developing their profiles.

But the servers came with a lot of cost starting from installation, maintenance to decommission. This problem was solved by the introduction of cloud computing. Cloud computing gave rise to database service providers where the developing organisation would just use their services and pay for the use. This was easier for them as now they just had to think about maintaining the application and not worry about maintaining the servers that would host the data.

As these database service providers made the job easier it led to another challenge. The challenge was how reliable were these service providers in terms of confidentiality of the data being stored in their database. Since, the data is with these providers it is difficult to know exactly how much accessible this data is to the outside world or how strongly are they securing the data being entrusted to them. This challenge can be overcome by encrypting the data being stored in the databases. Various techniques are used to ensure the security of this data and AES is one of the most widely used and highly trusted encryption algorithms. This way the data stored in these databases was secured from the outside world including the service providers.

II. SURVEY

Ako Muhamad Abdullah(2017)[1] states that because Advanced Encryption Standard (AES) algorithm makes it extremely difficult for hackers to get the real data when encrypted with it, it is the most common and widely used symmetric block cipher algorithm in the world. Three different key sizes such as AES 128, 192, 256 bits are provided by AEs and each cipher has 128-bit block size. Due to its own particular structure for encryption and decryption it finds application in both hardware and software world. No crack for this algorithm has been made evident till date. AES provides much more security in comparison to other algorithms like DES etc.

B. Iyer et al. (2002)[5] states with the rise of “software as a service” model due to advancements in networking and Internet technologies “Database as a Service” is providing its users with the power to create, store, modify and retrieve data around the world where an internet connection is available. The concern raised in the paper is what if the client does not trust the service provider. To this the solution discussed is to store

encrypted data in the database of the service provider which can be decrypted only by the owner i.e., decrypting of the data is performed only at the client site.

Zheng-Fei Wang et al. (2010)[4] states that traditionally, physical and operating system security were provided for database security but these were not enough support the security in the schema. Thus, cryptography was defined as a solution for database security. The authors define two parts for providing security to outsourced databases – Security Dictionary and extending of SQL. Development of a method to directly deal with the encrypted data before decrypting is stated along with key management.

Sharad Mehrotra et al. (2002)[2] state in the paper the various tasks involved in database management to be taken care by an organisation. These include expenses on hardware and software, software upgrades, migration of database and professionals for database maintenance, backup, restore etc. As a solution to all the above-mentioned tasks the authors introduce a new paradigm for data management – "Database as a service (DBaaS)". DBaaS is hosted by a third-party service provider providing services to create, store and access their database at the host site. Three challenges are mentioned by the authors. Firstly, data security needs to be focused upon, to which the solution is encryption. Secondly, performance should be evaluated and sources of degradation should be identified. Finally, an appropriate user interface should be provided that is easy to user but also provides resources for use.

Ajeet Ram Pathak et al. (2018)[3] states that Database as a Service has gained popularity in the world as a novel data management and administration paradigm. The security of outsourced databases is an important area of development for increasing the confidence of the clients. Concepts and benefits of Database as a Service have been discussed along with general security in outsourced database. Achievement of confidentiality, integrity, completeness, correctness, access control and accountability in single and multi-user environment has been discussed by authors in this paper.

Ankit Bansal et al. (2015)[6] have introduced approach to share information via an Android application between students and lecturers via HTTP technology . They Their project is related to the issues Faced by students in terms of academic resources and the notice circulation .They have designed and developed a mobile application for their campus which provide information regarding Departmental Details, Library Books Details, Placement Activities, General Notices, College Administration Details, Hostel Details ,Transportation Details And Admission Details. In their application student will be able to download study material (question, bank, assignment, notes, etc) and it can be used to find locations as well.

Chunnu Khawas et al,. (2018)[7] discussed how difficult it is for Relational Database Management System (RDBMS) to handle the unstructured data. Firebase is a relatively new technology for handling great amount of unstructured data. It is very fast as compared to RDBMS and the server used for Android apps are Oracle SQL, Microsoft SQL Server, and MySQL which are connected to the server with PHP files. Then Firebase came into existence for Android apps which use JSON for storing data. It helps developers‟ builds high-quality apps. It stores the data in (JSON) format. They have discussed about services available (Firebase Analytics, Firebase Cloud Messaging (FCM), Firebase Auth, Real-time Database, Firebase Storage, Firebase Test Lab for Android, Firebase Crash Reporting) and then conducted a comparison of various database and the steps to add firebase to android.

Divya Sharma et al. (2019)[8] discussed the sturdy infrastructure that is built with mobile backend services such as with Firebase which aids developers by handling the backend of these applications. In this paper ,The android application MCCApp showcase the features that are provide by Firebase and to show how it is best mobile backend-as-a-service and have done a comparison of Baas platforms material .Then they have discussed about the features of firebase Build better apps –Develop Products (Authentication, Realtime Database, Cloud Storage) ,Improve app quality – Quality Products (Crashlytics, Performance Monitoring, Test Lab) ,Grow your business – Grow Products(Remote Config, A/B Testing) and then demonstrate these feature by making a small app.

Rajivkumar Mente et al.(2017)[9] discussed the security of the applications and the malicious apps that may affect or leak sensitive data such as International Mobile equipment Identity Number (IMEI) of device, credit or debit card information, location information and so on. They discuss OS Application layer(Application framework layer, Libraries, Android Runtime-,Linux Kernel) and about android And its predefined set of

permissions, discussed about the Javed Parvez et al proposed Android Security Framework (AFS) which applies Advanced Encryption Standards (AES) algorithm to all the files stored in media and discuss how reverse engineering plays a role in security and vulnerability and the discussion of SSL/TLS (secured socket layer/transport layer security) and a conclusion that android provides good security but still, vulnerabilities and security problems arrive because of security flaws and improper development of the applications.

Sachin Patil et al. (2016)[10] discussed the difficulties that are generally faced by students and school regarding communication and correctness notifications their work revolves around notification and that they follow a hierarchical system concerning privileges, privileges are consistent with their designation or their types and have rights to post things on the application in order that other users can view that if they're alleged to or have permission to look at it. This feature is incorporated in their website not on android application. In their, android app which is employed only by the scholars. Nobody else has the access to the android application. Which may be a unidirectional communication.

Sunguk Lee (2012) [11] : This paper presents the review of Android tenets towards programming advancement for versatile(mobile) and non-portable applications. Android environments incorporate the well-known open-source SQLite database which has been utilized with extraordinary accomplishment as an "on-disk" document design that permits the developer to deal with information in a straightforward manner while likewise, having the utilization of database management system highlights (such as : redo, undo, and so forth). The principal for each Android application is its database support. A database framework is expected to store organized information. Android utilizes the SQLite database framework, it is a lightweight transactional or value-based database engine that possesses a small portion of disk space and memory. Subsequently, it is an optimal choice for developing databases on numerous mobile operating systems. It is implanted into the OS and supports standard information base highlights like transactions, SQL syntax structure, and prepared statements. Furthermore, it requires just little memory at runtime (approx. 250 KB).

K. Suresh et. al (2014) [12] : This paper discusses the pervasive data mining of databases from mobile devices by using web services. By allowing web services on mobile and other handheld devices, we buttress remote users to view sensitive data. They do this by executing data mining tasks from a mobile phone or a Personal Digital Assistant (PDA). As a large portion of developers and are familiar with Android now-a-days there lie possibilities of developing a mobile client application, a service oriented architecture platform based upon simple object access protocol (SOAP) messaging and JavaScript object notation (JSON) that can be used to strengthen the security of the system. This study focuses on the architectural alternatives, their impacts on the mobile client application with data mining applications, Android's performance on SOAP messaging, and how Web services' design can be optimized to give optimal performing Android clients.

S.R. Bharamagoudar et. al (2013) [13] : This paper involved The design and implementation of an elaborate student information system and the corresponding user-interface. This was done with an aim to replace the current paper and physical records that fill up office space and are generally a nuisance to manage efficiently. The creation and management of accurate, up-to-date information regarding a students' academic career is critically important in the universities. Student information system deals with an array of student details such as academic related reports, college details, course details, curriculum, batch details, placement details and other resource related details. It tracks all the information of a student from the day one to the end of the course. This can be used to keep a report of a student, track the attendance, see the progress being made in the course, completed semesters, the next year/semester curriculum details, exam details, projects being undertaken, assignment details among others. These will be available through a secure online interface embedded in the university website. Different reports and Queries can be generated based on vast options related to students, batch, course, faculty, exams, semesters, to name a few.

Jalal B. Hur, et. al (2017) [14] : This paper discusses the security risks and issues that are faced by Android run smartphones. In the last decade we have seen a paramount shift and increase in the number of people switching to smart phones in order to access the many features and applications in fields like finance, business, education and social, among others. Thus, making these devices the paramount target for hackers, however, on the other hand smart phone manufacturers are constantly trying to design the most efficient and ideal security model to overcome all vulnerabilities. Android security Architecture consists of the following components to

secure data with encryption and further, prevent malware. 1) Permission Mechanism: this mechanism provides an Android middleware layer. The interfaces vulnerable to security threats are protected by Android permission. It means that a certain application must have to gain prior permission from the user to perform operations such as making a call, accessing the internet and sending messages. 2) Sandboxing: this is a technique/security mechanism implemented to separate running applications. Each application has a unique identifier to access its own file. 3) Access Control: in access control, the mechanism of each file has an access rule and each process assigns a User ID. Each file has different access priorities for user, group and everyone. The process has a particular permission to read, write or execute the file. 4) Component Encapsulation: the components in a system are declared as private and public. Within the same application, private components are accessible for each other. The public components are accessible by other application which are not in the same sandboxing. 5) Application Signing: Android smartphones have an application signature that is verified via a cryptographic mechanism.

Lior Okman et. al (2011) [15] : With a meteoric rise in smartphone applications we have seen the need to store large amounts of data in distributed databases that provide high availability and scalability. A growing number of companies have begun to adopt various types of non-relational databases, commonly referred to as NoSQL databases, and as the applications they serve emerge, they gain extensive market interest. These new database systems are not relational by definition and therefore they do not support full SQL functionality. Moreover, as opposed to relational databases they trade consistency and security for performance and scalability. As increasingly sensitive data is being stored in NoSQL databases, security issues become growing concerns. This paper reviews two of the most popular NoSQL databases (Cassandra and MongoDB) and outlines their main security features and problems.

III. CONCLUSION

The aim of the survey is to put focus on application developed for colleges and security of the databases that store this data. In the present world, worth of data is increasing and also the data mining applications. So, to secure the necessary data stored in databases various encryption techniques can be used. The survey has discussed security risks in outsourced databases, android applications and also the techniques to implement and improve security.

IV. REFERENCES

[1] M. Abdullah, “Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data”, Cryptography and Network Security, 2017.

[2] H. Hacigumus, B. Iyer and S. Mehrotra, “Providing database as a service,” in Proc. of IEEE 18th ICDE, 2002, pp. 29-38.

[3] Ajeet R. Pathak, B. Padmavathi, “Survey of Confidentiality and Integrity in Outsourced Databases”, International Journal of Scientific Engineering and Technology, ISSN: 2277-1581. Vol. No.2, Issue No.3, pp. 122-128, 2018.

[4] Zheng-Fei Wang, Ai-Guo Tang, “Implementation of Encrypted Data for Outsourced Database”, In Proc. of Second International Conference on Computational Intelligence and Natural Computing (CINC), IEEE, 2010, pp. 150-153.

[5] H. Hacigumus, B. Iyer, C. Li, and S. Mehrotra, “Executing SQL over Encrypted Data in the Database-Service-Provider Model," SIGMOD'02, USA, 2002, pp. 216-227.

[6] Ankit Bansal, Ajit Rana, Akhil Bansod, Prafulla Baviskar (2015) , “Mobile Based Campus Information Retrieval Android Application” ,. IJCSMC, Vol. 4, Issue. 3, March 2015, pg.158 – 164.

[7] Chunnu Khawas, Pritam Shah “Application of Firebase in Android App Development-A Study” International Journal of Computer Applications (0975 – 8887) Volume 179 – No.46, June 2018.

[8] Divya Sharma, Hiren Dand “Firebase as BaaS for College Android Application” International Journal of Computer Applications (0975 – 8887) Volume 178 – No. 20, June 2019.

[9] Rajivkumar Mente and Asha Bagadi “Android Application Security” Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 10, Number 5 (2017)

[10] Sagar Rajebhosale, Mr. Shashank Choudhari, Mr. Sachin Patil, Mr. Akshay Vyavahare, Mr. Sanket Khabiya “SMART CAMPUS – An Academic Web Portal with Android Application” International

Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 04 | Apr-2016

[11] Sunguk Lee, "Creating and Using Databases for Android Applications", International Journal of Database Theory and Application Vol. 5, No. 2, June, 2012.

[12] K. Suresh E, Chaitanya krishna, Dr. K.Venkataramana, Prof. M. Padmavathamma, "Data Mining in Android Devices Through Web Services", International Journal of Engineering Research & Technology (IJERT) IJERT NCDMA - 2014 Conference Proceedings ISSN: 2278-0181.

[13] S. R. Bharamagoudar, Geeta R.B, S.G.Totad, "Web Based Student Information Management System", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 6, June 2013 ISSN (Print) : 2319-5940 ISSN (Online) : 2278-1021.

[14] Jalal B. Hur, Jawwad A. Shamsi, "A Survey on Security Issues, Vulnerabilities and Attacks in Android based Smartphone", 2017 International Conference on Information and Communication Technologies (ICICT) DOI: 10.1109/ICICT.2017.8320163.

[15] Lior Okman, Nurit Gal-Oz, Yaron Gonen, Ehud Gudes, Jenny Ab ra mov, "Security Issues in NoSQL Databases", 2011 International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11.