For relational databases i.e. Oracle SQL Server and MySQL, hackers may launch database attacks server, or bypass web server authentication using Injection SQL. Similarly, hackers will invade MongoDB uses JavaScript. Assault samples Started on MongoDB, seen in.

B.) Cassandra: The data files of Cassandra are stowed without encryption, and there is no automatic data encryption at the servers, it helps hackers to access the data that can be read straight away. Cassandra can handle Query Language in Cassandra (CQL) so that DBA can handle easily and clearly data inside database. This CQL does have a similar, Syntax as SQL's, so it is thought it could be attacked as with the SQL injection.
C.) CouchDB: CouchDB has no automatic encryption of the data as other NoSQL's, data archives are at risk retrieved directly, and read. In Contact Words among server and client, or between CouchDB servers, authentication is achieved by means of a system known as CRUD. Beside the communication, there is also an embedded SSL encryption which is a Compounding of CouchDB itself.
D.) Hypertable:
As with other, NoSQL's, there is no encryption at Hypertable the correspondence between the consumer and the server or between its servers is carried out for its data files without authentication, and encryption of data. Amazingly, Hypertable is free of injection vulnerabilities this has a data processing HQL, close to that of the Relational Database commands SQL.
E.) Redis: Redis does not sustenance data encryption in the same way as MongoDB and Cassandra, so the hackers or everyone with an access to the Redis server will indeed to retrieve all database data.

Not at all data encryption is carried out in the communiqué between the Redis client and the Redis server; In both supplementary servers, either on the same or different servers. Cluster, because Redis was designed primarily to function quickly, so there are not many components for its security. It is because of that reason that hackers have access to the network of Redis servers will be capable of detecting data while it's being conveyed.

Table 1. The Security Comparison of the Top 5 Open Source NoSQL Databases

Security Issues	Databases				
	MongoDB	Cassandra	CouchDB	Hypertable	Redis
Data files encryption	No encrypt	No encrypt	No encrypt	No encrypt	No encrypt
Client/Server Authentication /Encryption	weak	weak	SSL	No authen / No encrypt	No authen / No encrypt
Inter-cluster Authentication /Encryption	weak	weak	SSL	No authen / No encrypt	No authen / No encrypt
Script Injection	Vulnerable	Not vulnerable	Vulnerable	Not vulnerable	Not vulnerable
Denial of service attack	Not vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable

METHODOLOGY:

The technique for enhancing security through the use of database management is deponds on Encryption, a web-based solution. Server Protection, Adverse Registry, Authentication and Access Control, Timeliness and Control Safety in Real world Database Systems, SQL Injection Testing Schemes.

Encryption: This is the method of converting normal text info using encryption algorithms (called ciphers) that make it indecipherable to everyone but those with distinct features, Knowledge, which is usually referred to as the secret. Current database structures use plain text there are also risks of data manipulation and database failure. The data were used to stop these attacks. Stored in encrypted form.

Web-based Database Security: a range of methods are proposed to develop database security an unauthorized intrusion database. The transfer of data from the server to the client should be carried out using the Stable Socket Layer in a safe way. The Host Identity of the End Machine Regulated.

Deleterious Database: Negative data is applied to the original data in the database to avoid misuse of data from malevolent users and afford secure data recovery for all legitimate consumers.

Authentication and Access Control: Authentication is used to correctly verify the identity of the user. User and Access Management controls the behaviour or activities of the user. Access Control is given, Similar rights for specific authenticated users

Real-time Server Systems Timeliness and Security: Trade-off has to be made between the two. Security and transaction priority. Various approaches are suggested to ensure health and security have a small risk of exceeding time limits in real world database systems.

SQL Injection Testing Schemes: SQL Injection is a code inoculation technique that takes advantage of SQL Injections. A protection flaw that exists in the application's database layer.

CONCLUSION:

In this paper introduced a new framework for the execution of statistical analyses on interconnected data in a safe manner. Proposed method to make use of good protection of the privacy of RDBMS. This will make it possible to build stable assimilated infrastructures at a fair cost. A Secure and efficient Database Management System based on Integrated Statistical Data Analysis modelling and Privacy Preserving Analytics, first SAQeL prototype efficaciously exhibits the interface between DB2 and SAS.

REFERENCES:

[1] Barry, S., Marc, C.: remote access systems for microdata statistical review. Statistics and Computation 13 (2003) 381-389. See http:/www.lisproject.org as well.
[2] Borchsenius, L.: new innovations in the Danish Micro Data Access Method. Monographs on official statistics (2005) 13-20.
[3] Hibbert, M., Gibbs, P., O'Brien, T., Colman, P., Merriel, R., Rafael, N., Georgeff, M., Molecular Medicine Informatics Model (MMIM). Stud Health Techno Data 126 (2007) 77-86. See also: http:/www.biogrid.org.au.
[4] Hjelm, C.G.: MONA-Microdata ON-Access line at Statistics Sweden. Meta analyses on official figures (2005) 21-28. See http:/www.scb.se as well.
[5] SAS, http:/www.sas.com.
[6] DB2 Technology, http:/www.ibm.com/software/data/db2/.
[7] Sparks, R., Carter, C., Lehman, J.B., O'Keefe, C.M., Duncan, J., Keighley, T., McAullay, D.: Remote access approaches for excavation data processing and mathematical modelling: Privacy-Preserving Analytics. Computational methods Systems Biomed 91 (2008) 208-222.
[8] Haas, L.M., Lin, E.T., Roth, M.A.: Data fusion through database federation. It's IBM Syst. P. 41 › 2002 578-596.
[9] Luc, B., Fran, Oise, F., Fabio, P., Patrick, V.: Processing Queries for Costly Functions and Large Objects in Distributed Mediator Systems. The sessions of the 17th International Computer Engineering Conference. Computer Society of IEEE (2001) 91-98.
[10] Tisell, C., Orsborn, K.: A system for multibody analysis based on object-relational database technology. Advances in Engineering Software 31 (2000) 971-984.
[11] Ruslan, F., Magnus, S., Jan-Eric, L.: Federated Databases as a Basis for Infrastructure Supporting Epidemiological Research. Proceedings of the 2009 20th International Workshop on Database and Expert Systems Application. IEEE Computer Society (2009) 313-317.
[12] Stata: Data Analysis and Statistical Software, http://www.stata.com.
[13] The R Project for Statistical Computing, http://www.rproject.org.
[14] Open Database Connectivity Overview, http://support.microsoft.com/kb/110093
[15] Gayathri, A., Christy, S.”Image de-noising using optimized self similar patch based filter”,International Journal of Innovative Technology and Exploring Engineering, 2019, 8(12), pp. 1570-1578.
[16] Rama, A., Gayathri, A., Christy, S.”Fine tuning data mining algorithm for an efficient classification of E-coli”,International Journal of Innovative Technology and Exploring Engineering, 2019, 9(1), pp. 109-113
[17] Kumar Reddy, A.J., Gayathri, A., Mahalakshmi, D. “Automatic spam detection on twitter based on content and online social interaction”,Test Engineering and Management, 2020, 82(1-2), pp. 10603-10606.
[18] Reddy, K.N., Gayathri, A., Devi, T., “A primary warning methodology of train following interval supported government agency” Test Engineering and Management, 2020, 82(1-2), pp. 10499-10505.
[19] Manjusha, V., Gayathri, A., Logu, K., “Design of efficient multi-server password authenticated key management protocol for cloud computing environments”, Test Engineering and Management, 2020, 82(1-2), pp. 10493-10498.
[20] Reddy, M.H., Gayathri, A., Deepa, N. “An automatic method to prevent cybercrime incidents using artificial intelligence approach” ,Test Engineering and Management, 2020, 82, pp. 10488-10492.

AUTHORS PROFILE

Dr.A.Gayathri, received the B.E degree in Electronics and Communication Engineering from Periyar Maniammai College of Technology for Women (Bharathidasan University, India) in 2001 and the M.Tech (CSE) degree in Computer Science and Engineering specialization from Bharath University, Chennai, India in 2005. She completed the Doctorate in the Department of Information and Communication Engineering at Anna University. She is currently working as Associate Professor in Saveetha School of Engineering (Department of CSE), SIMATS, Chennai, and Tamil Nadu. She is the member of CSI, IAENG and ACM.

Dr.S. Thanga Revathi, working as Assistant Professor in SRM University of Science and Technology, Chennai. She has completed her Bachelor of Engineering degree in Computer Science and Engineering from Anna University, Chennai with distinction. She has completed her Master of Engineering in Computer Science and Engineering from Bharath University, Chennai. She completed her PhD in Anna University, Chennai and indulged in research work in the field of Data Security. She has a overall experience of 13 years in the field of Teaching. She has published papers in referred International and National journals. She has also presented papers in various National and International Conferences