# NoSQL verilənlər bazalarında təhlükəsizlik problemləri haqqında

Məkrufə Hacırəhimova[1], Mərziyə İsmayılova[2]
[1,2] AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]makrufa@scisence.az, [2]imarziya@google.com

***Xülasə*— Məqalə böyük verilənlər (“Big data”) və NoSQL verilənlər bazalarında təhlükəsizlik problemlərinə həsr olunmuşdur. Böyük həcm, sürət və müxtəliflik kimi xüsusiyyətlərlə xarakterizə olunan böyük verilənlərdə təhlükəsizlik və məxfilik ciddi problemlər yaradır. Ənənəvi təhlükəsizlik modelləri bu cür geniş miqyaslı verilənlərlə işləyən zaman çətinliklərlə rastlaşır. Məqalədə böyük verilənlər və NoSQL verilənlər bazalarında təhlükəsizlik və məxfilik problemləri araşdırılmışdır.**

***Açar sözlər:*** *böyük verilənlər, təhlükəsizlik, məxfilik, NoSQL, girişə nəzarət*

## I. GİRİŞ

Büyük verilənlər, daha səmərəli qərar qəbul etmə, informasiyanın aşkarlanması və proseslərin optimallaşdırılması üçün yeni emal formaları tələb edən böyük həcm, yüksək sürət və müxtəliflik kimi xüsusiyyətlərə malik informasiya resurslarını ifadə edir. Bəzən 3V kimi ifadə edilən xüsusiyyətlərinə görə ənənəvi verilənlər bazalarının idarəetmə alətlərindən istifadə etməklə böyük verilənləri emal etmək çox çətindir. Yeni bir çağırış - böyük həcmli verilənlərin geniş istifadəsi üçün yeni texnologiyalar və sistemlərin işlənib hazırlanmasıdır. Bu məqsədlə bir çox informasiya idarəedilməsi arxitekturları işlənmişdir [1, 2]. Bir çox sahələrdə yeni texnologiyaların inkişafı və böyük verilənlərdən istifadənin artması böyük verilənlərdə təhlükəsizlik və məxfilik kimi problemlərin yaranmasına səbəb olmuşdur. Böyük verilənlərə dair çoxlu sayda təhlükəsizlik və məxfilik problemləri mövcuddur [2 - 8].

İşin məqsədi böyük verilənlər və NoSQL verilənlər bazalarında təhlükəsizlik və məxfilik problemlərinin araşdırılmasından ibarətdir.

## II. BÖYÜK VERİLƏNLƏRDƏ TƏHLÜKƏSİZLİK PROBLEMLƏRİ

[7-9]-da böyük verilənlər üçün təhlükəsizlik və məxfilik üzrə on təhlükəsizlik problemi verilmişdir. Bu problemlər aşağıdakılardır:

- Paylanmış proqramlaşdırma strukturunda təhlükəsiz hesablamalar;
- Verilənlərin təhlükəsiz saxlanılması və tranzaksiya jurnalı;
- Girişə granular nəzarət;
- Girişin yoxlanması/filtirlənməsi;
- Real vaxt rejimində təhlükəsizliyin monitorinqi;
- Məxfiliyi saxlamaqla miqyaslama, verilənlərin əldə edilməsi və analizi;
- Kriptoqrafiya ilə həyata keçirilən girişə nəzarət və təhlükəsiz kommunikasiya;
- Qranular auditlər;
- Qeyri-relyason verilənlər bazaları üçün ən yaxşı təhlükəsizlik təcrübəsi;
- Verilənlərin mənşəyi.

Bu problemlərdən bir neçəsinin şərhi verilmişdir.

*Paylanmış proqramlaşdırma strukturunda təhlükəsiz hesablamalar problemi.* Bu MapReduce funksiyasında təhlükəsizliyi müzakirə edən bir problemdir. Verilənlərin təhlükəsiz saxlanılması və tranzaksiya jurnalı verilənlər anbarına icazəsiz girişin qarşısının alınmasını və girişin təmin edilməsinin yeni mexanizmlərini müzakirə edir.

*Girişə qranular nəzarət problemi*. Böyük verilənlərdə daha bir problem girişə granular nəzarət problemidir. Problem girişə ehtiyacı olmayan istifadəçilər tərəfindən verilənlərə girişin qarşısının alınmasındadır. Bu halda girişə nəzarətin ənənəvi modeli böyük verilənlərlə işləyərkən çətinliklə rastlaşır. [2 - 4, 12]-də böyük verilənlərin emalında girişə nəzarət üçün bir neçə mexanizm təklif edilmişdir.

*Verilənlərin mühafizə və girişə nəzarət problemi*. Böyük verilənlərdə təhlükəsizlik problemləri arasında verilənlərin mühafizəsi və girişə nəzarət daha mühüm problemlərdən sayılır. [13]-də NoSql VB-lər üçün qaydaya əsaslanan girişə nəzarətin (*Role Based Access Control, RBAC*) ənənəvi modellərini genişləndirmək yolu ilə girişin idarə edilməsi modeli təqdim edilmişdir. [14]-də NoSQL-in geniş istifadə olunan Cassandra və MongoDB VB-nin təhlükəsizlik problemləri müzakirə olunmuş, onların xüsusiyyətləri və təhlükəsizlik problemləri şərh edilmişdir. Cassandra və MongoDB üçün qeyd edilən əsas problemlər aşağıdakılardır:

- verilənlər faylının şifrələnməməsi;
- server və müştəri arasında zəif autentifikasiya;
- sadə autentifikasiya;
- SQL-inyeksiya və DOS hücumuna qarşı həssaslıq.

Həm də onların hər ikisinin RBAC və ətraflı avtorizasiyanı dəstəkləmədiyi bildirilir. [6]-da NIST risklərin

DOI: 10.25045/NCInfoSec.2018.54

idarə edilməsi standartları nəzərdən keçirilmiş və təhlükələrin mənbəyi, təhlükə hadisələri və zəifliklər müəyyən edilmişdir. Burada böyük verilənlərdə müəyyən olunmuş həssaslıqlar aşağıdakılardır:

- təhlükəli hesablama;
- girişin yoxlanılması/filtirlənməsi;
- girişə granular nəzarət;
- təhlükəli verilənlərin saxlanması və kommunikasiya;
- verilənlərin əldə edilməsinin məxfiliyinin qorunması və analizi.

Bəzi hallarda böyük verilənlərdə semantik məzmuna əsasən girişə nəzarət modelinə ehtiyac duyulur. Böyük verilənlərin paylaşılmasında giriş nəzarətini tətbiq etmək üçün, məzmuna əsaslanan giriş nəzarəti (*Content-Based Access Control, CBAC*) modeli verilənlərin məzmunundan istifadə etməklə təqdim olunur [2]. Bu halda, verilənlərin semantik məzmunu girişə nəzarət qərarının qəbul edilməsində əsas rol oynayır. CBAC məzmunların oxşarlığı əsasında istifadəçilərin qeydiyyat verilənləri və verilənlər arasında girişə nəzarət üzrə dinamik qərar qəbul edir [2].

[3] və [4]-də böyük verilənlərdə təhlükəsizliyi təmin edən digər bir metod - atributların qarşılıqlı əlaqəsi metodologiyası təklif edilmişdir. Bu metodologiyanın əsas məqsədi dəyərli informasiyaları mühafizə etməkdən ibarətdir. Ona görə də böyük verilənlərdə informasiyanın əldə edilməsi üçün açar elementi kimi atributların relevantlığına diqqət verilir və güman edilir ki, daha yüksək relevanlığa malik atribut digər atributlardan daha dəyərlidir. [3]-də modelin atributları və onlar arasındakı qarşılıqlı əlaqə üçün qrafdan istifadə edlir. Atributlar qovşaq kimi ifadə olunur və hər bir qovşaq arasında əlaqələr tillərlə göstərilir. Metod bu qraflardan mühafizə olunan atributların seçilməsini təklif edir. [4]-də təklif olunan metodda əvvəlcə verilənlərin bütün atributları əldə edilir, sonra xassələri ümumiləşdirilir. Daha sonra atributlar arasında korrelyasiya müqayisə olunur və qarşılıqlı əlaqə qiymətləndirilir. Nəhayət korrelyasiya qiymətləndirmələrinə əsaslanaraq təhlükəsizlik tədbirləri üzrə tələb olunan seçilmiş atributlar mühafizə olunur.

Bulud saxlama infrastrukturunda böyük verilənlərin girişinin idarə edilməsi üçün uyğun bir metod atribut əsasında şifrələmədir. [2]-də buludda böyük verilənlərin təhlükəsizliyini təmin etmək məqsədi ilə atribut şifrələmə əsasında effektiv girişin sxemi təklif olunur.

Hadoop böyük verilənlərin saxlanması və emalı üçün açıq kodlu strukturdur. Verilənlərin bir neçə qovşaqda saxlanması üçün Hadoop paylanmış fayl sistemindən (*Hadoop Distributed File System, HDFS*) istifadə edir. HDFS istifadəçinin autentikliyini yoxlamır, verilənləri şifrələmir və məxfiliyi təmin etmir. HDFS güclü təhlükəsizlik modelinə malik deyil və istifadəçilər birbaşa heç bir icazə olmadan qovşaqlarda saxlanan verilənlərə giriş əldə edə bilər [10]-da Hadoop-un bir neçə təhlükəsizlik riskləri qeyd edilmiş və verilənlərin saxlanması üçün girişin idarə edilməsinin yeni sxemi təklif olunmuşdur.

## III. NOSQL VERİLƏNLƏR BAZALARINDA TƏHLÜKƏSİZLİİK PROBLEMLƏRİ

***NoSQL (****Not Only SQL)* bu gün böyük verilənlər aləminin əsası hesab olunur və miqyaslana bilən müasir verilənlər bazaları (VB) üçün istifadə edilir. Miqyaslama –verilənlərin emalı baxımından tələbat artdıqda sistemin məhsuldarlığını artırma qabiliyyətidir. Böyük verilənlərin emalının dəstəklənməsi üçün platformalar miqyaslanmanın iki növünü: üfüqi və şaquli miqyaslama formasını nəzərdə tutur:

Üfüqi miqyaslamada iş yükü bir çox serverlər üzrə paylanır. Miqyaslamanın bu növündə buraxılış qabiliyyyətini artırmaq üçün bir çox system birləşir.

Şaquli miqyaslamada daha çox yaddaşlı prosessorlar və daha sürətli qurğular bir serverdə quraşdırılır [15].

Bu gün çoxlu sayda NoSQL həllər yaradılmışdır. [14]-də NoSQL-in əsas üstünlükləri aşağıdakı kimi təqdim edilmişdir: 1) sürətli şəkildə verilənləri oxumaq və yazmaq, 2) kütləvi saxlama, 3) asan genişlənmə, 4) aşağı qiymət. NoSQL sistemlərini dəstəkləyən verilənlər modeli açar-qiymət, sütun, sənəd və qraf kimi təsnif edilmişdir. Bu gün çoxlu sayda MongoDB, CouchDB, Redis, Voldermort, Cassandra, Hypertable, Hbase və Neo4j kimi. NoSQL həllər yaradılmışdır. NoSQL VB-lər verilənlər modelinə görə aşağıdakı kimi qruplaşdırılır [16-19]:

- Açar-qiymət - Cassandra, Voldemort, Redis, DynamoDB;
- Sənəd - MongoDB, CouchDB, DynamoDB;
- Sütun – HyperTable;
- Qraf – Neo4j.

*MongoDB* – sənədə əsaslanan NoSQL VB-dir və sənədlərin toplanmasını idarə edir. MongoDB mürəkkəb verilənlər tipini dəstəkləyir və böyük verilənlərə yüksək sürətli girişi təmin edir. MongoDB çevik, güclü, sürətli və istifadədə sadədir. Bütün verilənlər MongoDB-də mətn şəklində saxlanılır və verilənlər faylını şifrələmək üçün şifrələmə mexanizmi mövcud deyildir [15, 20]. Bu o deməkdir ki, fayl sisteminə giriş imkanı olan istənilən bədniyyətli istifadəçi fayllardan informasiya əldə edə bilər. O istifadəçi ilə MongoDB klasterləri və daxili avtorizasiya arasında təhlükəsiz əlaqə üçün X.509 sertifikatlı SSL istifadə edir. Lakin paylanmış rejimdə işə salındıqda autentifikasiya və avtorizasiyanı dəstəkləmir. Parollar MD5 heş alqoritminin köməyi ilə şifrələnir. Belə ki, MongoDB daxili skript dili kimi Javascript-dən istifadə etdiyi üçün inyeksiya (*ing. injection*) hücumuna məruz qalma imkanı vardır [14, 20, 21].

*CouchDB* – sənədə əsaslanan çevik, imtinaya davamlı NoSQL VB-dir. Bu açıq kodlu Apache layihəsidir və o HDFS-dən istifadə edir. CouchDB verilənlərin şifrələnməsini dəstəkləmir, lakin autentifikasiyanı həm parol, həm də *cookie* faylı əsasında dəstəkləyir. Parollar PBKDF2 heş alqoritmini tətbiq etməklə şifrələnir və SSL protokolundan istifadə edərək şəbəkə ilə ötürülür. Bu inyeksiya skriptləri və “xidmətdən imtina” hücumları üçün potensial imkana malikdir [14, 20, 21].

*Cassandra* – böyük verilənlərin idarə edilməsi üçün açıq kodlu paylanmış saxlancdır. Bu Facebook-da istifadə olunan

önəmli bir NoSQL VB-dir. Cassandra çeviklik, yüksək miqyaslama kimi xüsusiyyətlərə malikdir. Cassandrada bütün parollar MD5 heş funksiyası ilə şifrlənir, ancaq parollar çox zəifdir. İstənilən bir qərəzli istifadəçi qovşaqlar arasında mübadilədə avtorizasiya mexanizmi olmadığı üçün verilənləri asanlıqla əldə edə bilər. Cassandra “xidmətdən imtina” hücumları üçün açıqdır. Cassandra SQL inyeksiya üçün açıq olan Cassandra sorğu dili (*Cassandra Query Language, CQL*) adlanan sorğu dilindən istifadə edir [14, 16, 19-21].

*HBase* – Google böyük cədvəli əsasında yaranan və Java-da realizasiya olunmuş açıq kodlu sütun yönümlü VB-dir. O strukturlaşdırılmış və yarı strukturlaşdırılmış verilənləri idarə edir, paylanmış konfiqurasiya istifadə edir. Hbase qovşaqlar arası əlaqə üçün SSH (*Secure Shell)* protokolundan istifadə edir. O SASL (*Simple Authentication and Security Layer*) və həm də ACL (*Access Control List*) vasitəsilə ilə istifadəçi avtorizasiyasını dəstəkləyir [20].

NOSQL VERİLƏNLƏR BAZALARININ MÜQAYİSƏSİ

| NoSQL VB | Verilənlərin tipi | Autentifikasiya | Avtorizasiya | Verilənlərin məxfiliyi | Audit | Əlaqə protokolu | Hücum üçün potensial imkan |
|---|---|---|---|---|---|---|---|
| MongoDB | Sənəd | Dəstəklənmir | Dəstəklənmir | Dəstəklənmir | - | SSL | Script inyeksiyası |
| CouchDB | Sənəd | Dəstəklənir | - | Dəstəklənmir | - | SSL | Script inyeksiyası və DOS |
| Cassandra | Açar-qiymət | Dəstəklənir | Dəstəklənmir | Dəstəklənmir | Dəstəklənmir | SSL | Script inyeksiyası (CQL)-də və DOS |
| Hbase | Sütun | Dəstəklənir | Dəstəklənir | Dəstəklənmir | - | SSH | DOS və inyeksiya üçün hesabat yoxdur |
| HyperTable | Sütun | Dəstəklənmir | - | Dəstəklənmir | - | - | - |
| Voldemort | Açar-qiymət | Dəstəklənmir | Dəstəklənmir | Dəstəklənir | Dəstəklənmir | - | - |
| Redis | Açar-qiymət | Kiçik lay | Dəstəklənmir | Dəstəklənmir | Dəstəklənmir | Şifrələnməmiş | - |
| DynamoDB | Açar-qiymət Sənəd | Dəstəklənir | Dəstəklənir | Dəstəklənmir | - | https | - |
| Neo4j | Qraf | - | Dəstəklənmir | Dəstəklənmir | Dəstəklənmir | SSL | - |

*HyperTable* – HDFS-də istifadə olunan açıq kodlu yüksəkməhsuldarlı sütun yönümlü VB-dir. O verilənləri böyük cədvəllərdə saxlayır. Hypertable verilənlərin şifrələnməsi və autentifikasiyanı dəstəkləmir. Əgər hər hansı bir server sıradan çıxarsa verilənlər bərpa edilmir. HyperTable inyeksiya hücumları üçün açıq olan HyperTable sorğu dili (*HyperTable Query Language, HQL*) istifadə edir. DOS hücumlara məruz qalmır [21].

*Voldemort* – Linkedin-də istifadə olunan “açar-qiymət” tipli NoSQL VB-dir. Bu tip VB-də verilənlər “açar-qiymət” cütlüyü şəklində saxlanılır. O, saxlama mexanizmi kimi Berkeley DB-dən istifadə etməklə verilənlərin şifrələnməsini dəstəkləyir. Voldemort autentifikasiya, avtorizasiya auditi dəstəkləmir [22].

*Redis* – “açar-qiymət” tipli açıq kodlu VB-dir. Redis-də verilənlərin şifrələnməsi dəstəklənmir və bütün verilənlər mətn şəklində saxlanılır. Redisin müştəriləri ilə server arasında əlaqə şifrələnmir. Redis-də kiçik bir səviyyədə autentifikasiyını təmin edən girişə nəzarət həyata keçirilmir. Redis-də inyeksiya hücumu imkansızdır [21].

*DynamoDB* – Amazonda istifadə olunan sürətli və çevik NoSQL VB-dir. O həm “açar-qiymət”, həm də sənəd verilənlər modelini dəstəkləyir [21]. DynamoDB-də verilənlərin şifrələnməsi dəstəklənmir, lakin müştəri və server arasında verilənlərin mübadiləsi https protokulundan istifadə edir. Autentifikasiya və avtorizasiya DynamoDB tərəfindən dəstəklənir [22].

*Neo4j* - açıq kodlu qraf yönümlü NoSQL VB-dir. Neo4j verilənlərin şifrələnməsini, avtorizasiya və auditi dəstəkləmir. Müştəri və server arasında əlaqə SSL protokoluna əsaslanır [22].

## NƏTİCƏ

Böyük verilənlər və NoSQL VB-lərlə işləyən zaman təhlükəsizlik çox önəmlidir. NoSQL VB-lərdən istifadə artdıqca təhlükəsizlik daha ciddi problemə çevrilir. Məqalədə böyük verilənlərdə və NoSQL verilənlər bazalarında (MongoDB, CouchDB, HyperTable, DynamoDB və s.) təhlükəsizlik və məxfilik problemləri şərh edilmişdir. Böyük verilənlərin böyük həcm, sürət və müxtəliflik kimi xüsusiyyətlərindən asılı olaraq ənənəvi təhlükəsizlik modelləri səmərəsizdir. Bəzi tədqiqatçılar böyük verilənlər üçün yeni – girişə nəzarət modelini təqdim etmişdirlər. NoSQL VB-lərin əksəriyyəti verilənlərin şifrələnməsini dəstəkləmir. Bu da təhlükələrin yaranmasına zəmin yaradır. Yuxarıda qeyd edildiyi kimi daha təhlükəsiz VB-yə malik olmaq üçün VB-nin məxfi sahələrinin şifrələnməsi vacibdir. Bəzi VB-lərin inyeksiya üçün zəifliyi var. Onlardan bəziləri autentifikasiya mexanizminə, bəziləri isə zəif autentifikasiya mexanizminə malikdirlər. Bu çatışmazlıqları aradan qaldırmaq üçün güclü autentifikasiya mexanizmləri lazımdır.

Yuxarıda cədvəldə bu müqayisələr təqdim edilmişdir.

## ƏDƏBİYYAT

[1] R.Əliquliyev, M.Hacırəhimova “Big data” fenomeni: problemlər və imkanlar // İnformasiya Texnologiyaları Problemləri, 2014, №2, s. 3–16.

[2] K.Yang, Secure and Verifiable Policy Update Outsourcing for Big Data Access Control in the Cloud, IEEE Transactions on Parallel and Distributed Systems, 2014, Issue 99.

[3] W.Zeng, Y.Yang, B.Lou, Access control for big data using data content / Proceedings of the IEEE International Conference on Big Data, 2013, pp. 45-47.

[4] S.Kim, J.Eom, T.Chung, Big Data Security Hardening Methodology Using Attributes Relationship / Proceedings of the IEEE International Conference on İnformation Scence and Applications, 2013, pp. 1-2.

[5] S.Kim, J.Eom, T.Chung, Attribute Relationship Evaluation Methodology for Big Data Security / Proceedings of the International Conference on IT Convergence and Security (ICITCS), 2013, pp. 1-4.

[6] M.Paryasto, A.Alamsyah, B.Rahardjo, Big-data security management issues / Proceedings of the International Conference on Information and Technology (ICoICT), 2014, pp. 59-63.

[7] R Alguliyev, Y. Imamverdiyev Big Data: Big promises for information security / Proceedings of the IEEE 8th International Conference on Application of Information and Communication Technologies (AICT), Astana, Kazakhstan 15-17 October, 2014, pp.216–219.

[8] R.Əliquliyev, F.Abdullayeva Bulud texnologiyalarının təhlükəsizlik problemlərinin tədqiqi və analizi // İnformasiya Texnologiyaları Problemləri, 2013, №1, s. 3–14.

[9] Cloud Security Alliance, Cloude Top Ten Big Data Security and Privacy Challenges, 2013, www.cloudsecurityalliance.org.

[10] A.Jha, M.Dave, S.Madan, Big Data Security and Privacy: A Review on Issues, Challenges and Privacy Preserving Metods // International Journal of Computer Applications, 2017, vol. 177, no 4, pp. 23-28.

[11] M.Hacırəhimova, “Big Data” texnologiyaları və informasiya təhlükəsizliyi problemləri // İnformasiya Texnologiyaları Problemləri, 2016, №1, s. 49–56.

[12] C.Rong, Z.Quan, A.Chakravorty, On Access Control Schemes for Hadoop Data Storage / Proceedings of the International International Conference on Cloud Computing and Big Data, 2013, pp. 641-645.

[13] M. Shermin. An access control model for NoSQL databases. Master’s thesis, University of Western Ontario, 2013. http://ir.lib.uwo.ca/etd/1797.

[14] L.Okman, N.Gal-Oz, Y.Gonen, E.Gudes, J.Abramov, Security Issues in NoSQL Databases / Proceedings of the IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2011, pp 541-547.

[15] D.Singh, C.K.Reddy, A survey on platforms for big data analytics // Journa of Big Data, 2014, pp.2-8.

[16] J. Han, E. Haihong, G. Le, and J. Du, “Survey on nosql database” / Proceedings of the IEEE International Conference in Pervasive Computing and Applications (ICPCA), 2011, pp. 363–366.

[17] R. Cattel, Scalable SQL and NoSQL data stores. ACM SIGMOD Record, 2010, vol. 39 no 4, pp. 12-27.

[18] A. Siddiqa, A. Karim, A. Gani, Big data storage technologies: a survey // Frontiers of Information Technology & Electronic Engineering, 2017, vol. 18, no 8, pp. 1040-1070.

[19] Strauch C. NoSQL Databases. http://www.christof-strauch.de/nosqldbs.pdf.

[20] A.Zahid, R.Masood, M.A.Shibli, Security of Sharded NoSQL Databases: A Comparative Analysis / Proceedings of the Conference on Information Assurance and Cyber Security (CIACS), 2014, pp 1-8.

[21] P.Noiumkar, T.Chomsiri, A Comparison the Level of Security on Top 5 Open Source NoSQL Databases / Proceedings of the International Conference on Information Technology and Applications(ICITA2014), 2014

[22] K.Grolinger, W.A.Higashino, A.Tiwari, M. AM Capretz, Data management in cloud environments: NoSQL and NewSQL data stores // Journal of Cloud Computing: Advances, Systems and Applications, 2013, vol. 2, no1, pp. 2-24.

## ABOUT SECURITY PROBLEMS IN NOSQL DATABASE

Makrufa Hajırahimova[1], Marzıya Ismayılova[2]

[1,2] Institute of Information Technology of ANAS, Baku, Azerbaijan

[1]*makrufa@scisence.az*, [2]*imarziya@google.com*

**Abstract** -- The paper is dedicated to security issues in big data and NoSQL databases. Big data, characterized by features such as large volume, velocity, and variety, make serious problems for security and privacy. Therefore, traditional security models have difficulties in dealing with such large scale data. In this paper, security and privacy issues have resarched in big data and NoSQL databases.