International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Review on Network Privacy Information Security Management Method based on NOSQL Database

Siddhesh Vijay Patil [1], Atharv Makarand Relekar[2], Prof. V.M.Lomte[3]

[1]*Computer Engineering Student, R.M.D.Sinhgad School of Engineering, Pune, Maharashtra, India*
[2]*Computer Engineering Student, R.M.D.Sinhgad School of Engineering, Pune, Maharashtra, India*
[3]*Head of department of Computer Engineering, R.M.D.Sinhgad School of Engineering, Pune, Maharashtra, India*

Abstract - *With the increasing user need the data is increasing day by day. Hence to store and manage such huge data the big databases like Oracle, MongoDB, NoSQL, etc can be used. NoSQL is the most widely used among all. Although some companies prefer to use relational databases depending on data being stored. It is very much necessary to secure such huge data from various threats with proper methods. This paper focuses on various issues related to databases and various solutions to protect data from such threats.*

Key Words: *NOSQL database, Network Privacy, Information security, Safety management.*

Motivation: In today's world, security is the most important concern. With the increasing data and crime it is becoming more and more difficult to manage security of data. The data if misused can result in many drawbacks. A person's money can be withdrawal by a hacker, of which bank is unknown resulting in loss of customer's money. A hacker can misuse private information of a person. A hacker can also destroy any organization, if security is not managed properly. Hence proper security of data is the important factor to be concerned.

1. INTRODUCTION

Nowadays, with the increasing population and technology the demand for data storage and retrieval is increasing day by day. Organizations even keep backup of their data for use, if current data is lost due to some problem. Thus data is increasing day by day, as data is the most important aspect of todays world. For storage of unstructured data NoSQL database can be used. NoSQL database systems provide real time performance while managing huge data. The data structures used by NoSQL are different than those used by the relational databases. If the data is changing over time, NoSQL is best choice to be used. However security of data is the most important concern.

NoSQL database are at evolutionary stage, unlike relational databases. The attack vectors for NoSQL are not well mapped out. There is a high possibility that new attack vectors will emerge on NoSQL [1]. To overcome this problem researchers are coming with new ways. The best practice to secure data can be, firstly access the privacy information security and prepare security evaluation architecture to analyze security evaluation index. Then encrypt network privacy information. After encryption implement security management by verifying the user by calculating the trust value. Thus data can be secured. This method proves to be best as compared to the traditional method. However this method take long security protection time and has low efficiency. Thus more research needs to be carried out regarding the security.

2. LITERATURE SURVEY

Table -1: literature survey

Sr.no	Published year	Published by	Research topic	Access Parameter	Outcomes
1.	2016	1.Toru Mano, 2.Takeru Inoue, 3.Dai Ikarashi, 4.Koki Hamada 5.Kimihiro Mizutani, and 6.Osamu Akashi	Efficient Virtual Network Optimization across Multiple Domains without computation (MPC) .	1.service providers (SPs) and infrastructure providers (InPs) 2. Multi-party computation (MPC).	Optimized virtual network on multiple domains

Sr. no	Published year	Published by	Research topic	Access Parameter	Outcomes
2.	2017	1.Boyu Hou 2.Yong Shi 3.Kai Qian	Towards Analyzing MongoDB NoSQL Security and Designing Injection Defense Solution . [13]	1.Input validation limit 2.Assign permission to the users 3.Check and filter variables 4. Malicious Feature Detection.	Demonstrated sever side javascript and HTTP injection attacks and propose defence methods
3.	2017	1.Shan Dong 2.Xu Xinzheng	Multi-label learning model based on multi-label radial basis function neural network.[3]	Network privacy information management model.	This method can complete the security for small network privacy
4.	2017	1.Li Dianwei, 2.He Mingliang, 3.Yuan Fang	Research on Insider Threat Detection Based on Role Behavior Pattern Mining[J]. [4]	Internal threat detection model.	domestic threat detection model is theoretically feasible
5.	2017	1.Jitender Kumar 2.Varsha Garg	Security analysis of unstructured Data in NoSQL MongoDB database. [14]	data is encrypted before storing in database and decrypted after accessing from the database.	Blowfish encryption or decryption algorithm is giving better performance than AES and DES. AES is most suited to apply to the client-server architecture in MongoDB.
6.	2017	1.Xu Guangxian 2.Zhao Yue 3.Public Zhong Sheng	Design of Double Encryption security network coding scheme based on chaotic sequence. [5]	Encrypts the data chaotically.	reduces the possibility of information leakage.
7.	2017	1.Alfredo Cuzzocrea 2.Hossain Shahriar	Data Masking Techniques for nosql Database Security: A systematic review. [15]	Masking Techniques: 1.Substitution 2.Shuffling 3.Number and date variance 4.Deletion 5.Masking out 6.Hashing 7.Encryption	Provides extensive overview of various vulnerabilities in mongoDB and Cassandra. Study of different data masking techniques.
8.	2018	1.Zhu Xiaoyan, 2.Zhang Hui 3.Ma Jianfeng.	Android Platform Privacy Protection System Based on Hook Technology [8]	achieve dynamic monitoring and intercept malicious application acquisition	reduces the false alarm rate while ensuring the detection of collusion attacks
9.	2018	1.Kosovare Sahatqija 2.Jaumin Ajdari 3.Xhemal Zenuni 4.Bujar Raufi 5.Florije Ismaili .	Comparison between relational and NOSQL databases [16]	1.NoSQL database 2.Relational Databases.	With ACID properties, relational database are the appropriate choice. If there are large datasets, then NoSQL is the perfect solution.

10.	2019	1.Md Rafid Ul Islam 2 Md. Saiful Islam 3. Zakaria Ahmed 4. Anindya Iqbal 5. Rifat Shahriyar.	Automatic Detection of NoSQL Injection Using Supervised Learning [17]	1.Training Dataset Generation 2. Feature Design 3. Feature Selection(10 features)	Automated system to detect NoSQL threats
11.	2019	1.Murat Kantarcioglu 2. Fahad Shaon.	Securing Big Data in the Age of AI [18]	1.Enforce Policies 2.Keep audit logs 3.Sanitize data 4.Detect Unauthorized access 5.automatically create policies	Data security and privacy tool overview for data security

3. ALGORITHMIC SURVEY

Table -1: Algorithmic survey

Sr.no	Access Parameter	Algorithm	complexity
1.	1.service providers (SPs) and infrastructure providers (InPs) 2. multi-party computation (MPC). [12]	1.Selecting Optimal Virtual Network by Service Provider 2. Enumerating Virtual Network Pieces by Infrastructure Providers	1.O(n) 2.O(n)
2.	1.Input validation limit 2.Assign permission to the users 3.Check and filter variables 4. Malicious Feature Detection.[13]	-	-
3.	Network privacy information management model. [3]	1.nearest neighbor propagation clustering algorithm 2.ML-RBF 3.AP clustering algorithm	1.O(logn) 2.O(nSV)*d nSV is number of support vectors D is input dimensionality 3.O(N^2T)
4.	internal threat detection model.[4]	-	-
5.	data is encrypted before storing in database and decrypted after accessing from the database. [14]	1.Data encryption standard 2.Asvanced Encryption Standard 3. Blowfish 4. symmetric cryptographic algorithms	1.O(k), where k depends on hardware used 2.O(k) 3.O(k) 4.O(k)
6.	Encrypts the data chaotically.[5]	1.Linear Network Encoding 2.Chaotic sequence 3. Sink decoding	1.O(2B+1)h^2k^2 O(h^2*(√T+h+l)
7.	Masking Techniques: 1.Substitution 2.Shuffling 3.Number and date variance 4.Deletion 5.Masking out 6.Hashing 7. Encryption. [15]	-	-
8.	achieve dynamic monitoring and intercept malicious application acquisition.[8]	1.data mining classification 2.Hook technology	1. O(n) 2.Depends on software
9.	1.NoSQL database 2.Relational Databases. [16]	-	-
10.	1.Training Dataset Generation 2. Feature Design 3. Feature Selection(10 features) [17]	1.K-nearest neighbor 2.Greedy stepwise search	1.O(nm) 2.O(b^m)
11.	1.Enforce Policies 2.Keep audit logs 3.Sanitize data 4.Detect Unauthorized access 5.automatically create policies [18]	-	-

4. CONCLUSION

In summary, after the study of various methods and algorithms we find that data encryption and verification can be used for secure data management, but still the research has some shortcomings. Hence there is need for more research to be carried out for security of data.

5. REFERENCES

[1]https://www.computerweekly.com/tip/Securing-NoSQL-applications-Best-practises-for- big-data-security.

[2] Mu Qi. "On the Management Analysis of Big Data and Network Information Security [J]". Information Records 2018, 19(9):51-52.

[3] Shan Dong, Xu Xinzheng."Multi-label learning model based on multi-label radial basis function neural network and regularized extreme learning machine[J]". Pattern Recognition and Artificial Intelligence, 2017, 30(9):833-840.

[4] Li Dianwei, He Mingliang, Yuan Fang. "Research on Insider Threat Detection Based on Role Behavior Pattern Mining[J]". Netinfo Security, 2017, 25(3):27-32.

[5] Xu Guangxian, Zhao Yue, Gong Zhongsheng. "Design of secure network coding scheme by double encryption based on chaotic sequences[J]". Journal of Computer Applications, 2017, 37(12):3412-3416.

[6] Ma Rong. "Analysis on Key Technologies of Network Information Security Management [J]". Information Technology and Informatization, 2017, 11(9):102-104.

[7] Mie Weizeng. "lication of Virtual Private Network Technology in Computer Network Information Security [J]".Computer Knowledge and Technology,2017, 13(4):28-29.

[8] Zhu Miaoyan, Zhang Hui, Ma Jianfeng." Android Platform Privacy Protection System Based on Hook Technology [J]". Journal of Network and Information Security, 2018, 29(4):42-51.

[9] Liu chi." Research on Network Security and Privacy Protection in the ConteMt of Big Data [J]". Modern Communication, 2018, 491(21):58-59.

[10] Lu Yue, Chen Miuzhen, Ma Jin. "Social Network Hierarchical Privacy Protection Algorithm Combining Community Partition [J]". Communication Technology, 2018, 51(2):404-412.

[11] Min Ying." Discussion on Network Information Security Protection Strategy in Data Age [J]". Network Security Technology and lication,2018, 212(8):60+81.

[12] Toru Mano, Takeru Inoue, Dai Ikarashi, Koki Hamada, Kimihiro Mizutani, and Osamu Akashi. "Efficient Virtual Network Optimization across Multiple Domains without Revealing Private Information". IEEE Transactions on Network and Service Management, sept 2016.

[13] Boyu Hou, Yong Shi, Kai Qian. "Towards Analyzing MongoDB NoSQL Security and Designing Injection Defense Solution". 2017 IEEE 3rd International Conference on Big Data Security on Cloud.

[14] Jitender Kumar, Varsha Garg. "Security analysis of unstructured data in Nosql MongoDB database". 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN).

[15] Alfredo Cuzzocrea, Hossain Shahriar."Data Masking Techniques for nosql Database Security:A systematic review".2017 IEEE International Conference on Big Data (BIGDATA).

[16] Kosovare Sahatqija, Jaumin Ajdari, Xhemal Zenuni, Bujar Raufi, Florije Ismaili. "Comparison between relational and NOSQL databases".2018 41st International Convention on information and communication technology, electronics and microelectronics.

[17] Md Rafid Ul Islam, Md. Saiful Islam, Zakaria Ahmed, Anindya Iqbal, Rifat Shahriyar. "Automatic Detection of NoSQL Injection Using Supervised Learning". 2019 IEEE 43rd Annual Computer software and Applications Conference(COMPSAC).

[18] Murat Kantarcioglu, Fahad Shaon. "Securing Big Data in the Age of AI". 2019 First IEEE International Conference on Trust, Privacy and Security in Intellingent Systems and applications (TPS-ISA).