THE ENHANCEMENT OF BIG-DATA SECURITY USING MULTI DIMENSIONAL USER ACCESS

J. Gowtham

Department of Computer Science and Engineering, Mahendra College of Engineering and Technology, India

Abstract

The Big data refers to a process used when traditional data mining and manipulation techniques could not detect the ins and outs of basic data. The Un-configured or time sensitive or simply very large data cannot be processed by associated database machines. This type of data requires a different processing approach called big data, which utilizes massive parallelism in the readily available hardware. The big data security refers to the security digital privacy measures used to prevent unauthorized access to computers, databases and websites. The big data protection also protects data from corruption. The big data security is an important aspect of IT for companies of every size and type. In this paper an enhanced security model was proposed to improve the security of the big data services. While the multi users are approach a single data set in the database, there may be collusion occurs between the users. There we need to enhance the security. The proposed method improves the security of the user access in various sessions.

Keywords:

Big Data, Database Machines, Massive Parallelism, Hardware, Big Data Security, Big Data Protection

1. INTRODUCTION

Quite simply, big data reflects the world we live in. As more and more things change, changes are captured and recorded as data. For a weather forecaster, the amount of data collected worldwide regarding local conditions is substantial. Logically, local contexts dictate regional effects and regional effects dictate global effects, but this may be the other way around.

One way or another, this meteorological data reflects the properties of large data, where a large amount of data requires real-time processing, and the machine can generate a large number of inputs, such as individual observations or external forces such as solar points [1]-[2].

Processing information like this explains why big data is so important:

- Most of the data collected now is unstructured and requires different storage and processing than found in traditional related databases.
- The available computing power is sky-rocketing, which means there are more opportunities to process big data.
- The internet has democratized data, increasing data steadily, and generating more and more raw data.

Data in its original form has no value. Data must be processed to be valuable. However, there is an inherent problem with big data here. Is it worth the huge capital cost to process data from own object design to usable intelligence? Or is there too much data with unknown values to justify gambling to implement it with big data tools? Most of us agree that if the weather is predictable there will be value; the question is whether that value will outweigh the costs of crushing all real-time data. Researchers using traditional data mining have been manipulating data for many years. The same analysts now find it difficult to cope with the amount and variety of data stored by businesses, private companies and government agencies [3]-[7].

The Small data captured data are unique and accurate enough for the human brain to understand. Typically, it is collected for a specific purpose per unit of an organization, i.e. to record how much real effort is expended on different activities by individuals within a group. The reason for collecting small data is initially established. In this case, it will be collected with the aim of improving how a team presents its value. In comparison, the focus of big data is to gather as much relevant information as possible across the company and then analyze how it might help to answer questions. What do our sales figures say about market trends and additional sales opportunities. Its good is our support team at handling customer queries. It should we improve our project distribution process to reduce excessive costs against the estimated budget. It may seem obvious, but big data requires input data, and there is a lot of it [8]. The answers to the initial questions raise many more as more small data is needed to support the larger data. In addition, there are numerous enterprise-wide tools provided by sellers to analyze this information, tools that require significant investment and time to bring home, configuration and configuration to begin delivering results. It is a computer integration program from the beginning to connect to all sources of data and can take months to deliver business benefit.

Conversely, small data requires little analysis, and can be captured in a number of temporary ways, such as spreadsheets, work and time tracking tools, and manual record books, and analyzed quickly and easily. I found that within a week or two of the start of productivity engagement the benefits from small data were realized. That's because it takes a while to capture source information. In general, changes and benefits are quickly seen due to the focus of the data collected [9].

2. LITERATURE REVIEW

This is the digital world. Everything here is data. There is a huge market here for the personal data you give away. You are laying the groundwork for someone to run you, knowingly or unknowingly. They get at least some information from you no matter which website you go to. Service providers will collect from your basic information such as where you use the service, what tools you use it for, and when you use it the most [6]. Usually Facebook, like your email, collects more data from you such as date of birth and destination. Any company collects this data to provide their service to the users accordingly. This is called `Data Analytics`. That is, they lay out a model for a user based on the data they receive. So, we need to focus on what kind of service site we use and what kind of information it receives from us. A website should not collect personal data such as your name or age.

Those in this area need to collect general data such as who is using this information the most at this time [7].

If a company keeps collecting data from you and is able to identify you as you it is a violation of individual rights. Both problems are more likely to occur when providing more data. One is sharing more of your personal information with third parties than is necessary. Second you give them the opportunity to spend more time on their website or processor with the data you provided. You also need to be careful about the data you give to social media accounts. Whether it's your email or your birthday [9]. Similarly, when we download a processor, we need to test whether we are doing it from a trusted site. You need to understand that it is not necessary for any person who is not related to you to know excessive data about you [10]. Thus, not only when providing data but also when sharing photos, you need to focus on what kind of message you are conveying to the outside world by the photo taken from where it came from. By posting photos of airline tickets, photos we take from our home, places we go to, it means that we release our personal information to the public without our knowledge.

3. PROPOSED METHOD

The proposed big data security algorithm (BDSA) has unique growth of the corporation presents key data security challenges for big data managers. The old one is that data storage techniques are not suitable for large databases that are not configured. These play an important role in business intelligence (PI), functional intelligence, marketing and more. All this data processing companies need to hire new tools, solutions and staff. Because data are drawn automatically from data, the integrity of big data is very important. But no matter how much time and money companies spend on data management, big data collection, storage and processing, there are still additional costs with its security. Information Security does not just about know that your data is secure. It meets the requirements for storage and knowing that you have done everything in your power to protect your data.

The big data security is also known as information security (IS) or system security. Examples of data protection technologies include backups, data encryption and data erasure. An important data protection technology is encryption, where digital data, software / hardware and hard disks are encrypted, making them unreadable to unauthorized users and hackers. One of the most commonly encountered methods for practicing data security is the use of authentication. With authentication, users must provide a password, code, biometric data or some other data to verify identity before being granted access to a computer or data. The Data protection is also very important for health care records, so health consultants and medical practitioners in the United States and other laboratories, clinics, hospitals, and other medical facilities. One reason security structure and security design often go in the same sentence is that flexibility uses resources (architecture) to implement concept (design) in effective ways that protect both data in use. It spreads through a computer) and residual data (archived data.)

- **Data Protection**: It is mandatory to visit a site you need to be careful about what kind of data you provide.
- **Mail Protection**: If your email address is not requested then you do not need to provide it. If no email is required, you will need to keep an email to give to the public as well as an email for your personal use.
- **VPN Protection**: Some people think that if they use VPN their data will not be known to any particular service site. But it is not so. When you use VPN, only the companies that provide you internet access will be unaware of it. If you log in and sign in to the website you are using, it means that you have given your data.
- **Incognito Protection**: If we use some processors for a limited period of time, we can provide temporary data for it. Similarly in the incognito window your data will not be stored on the computer but will definitely go to the website you are using. Asking if the information you give to use such processors is misused is more likely to say so.

IT professionals use a variety of policies and ideas to address security design. Some examples are the use of conceptual security domains or levels, where creating a wide gap between an elite administrator and a large number of users is one way to protect an organization. Direct monitoring and control of data in use are common security design elements. IT professionals can talk about stacking or shrinkage as additional design elements, where separating different parts of a security structure can provide better security and shrinkage, or prevent some kind of reverse engineering that can lead to closed door engineering security breaches.

4. RESULTS AND DISCUSSION

The proposed big data security algorithm (BDSA) was compared with the existing. An efficient time optimized scheme (ETOS), Big data frontier for innovation (BDFI), Privacy preserving processing of data decision (PPPD) and Accelerated PSO swarm search (PSOS)

Compliance is a catch-all term, i.e., you set internal policies (corporate data governance policies) and external rules (specific restrictions on the organization of your partners and branch organizations such as the EU, government, credit card companies). These meet many requirements, and many costs that are not very clear. Here are some examples of what data management and regulatory compliance can cost your organization. These are the expenses you have incurred.

Table.1. Compression of Protection of data governance policies

Security Selection Instructions	ETOS	BDFI	PPPD	PSOS	BDSA
100	58.01	61.41	85.44	79.23	95.19
200	56.34	60.28	82.51	77.97	92.72
300	54.39	59.93	80.97	76.08	91.92
400	52.40	57.98	78.94	74.88	90.72
500	49.82	57.21	78.04	83.32	90.08
600	47.83	56.83	76.07	71.57	88.82
700	45.81	55.70	74.60	70.64	87.82

We will hire overseas or internally trained professionals. With both options you have to spend to train for changes that do not change during any of the terms. Compliance with the rules

requires a data manager within the organization who is well versed in the regulations. He knows how to meet integrity needs. This often means hiring new skills from outside or training internally. Either way, these security professionals need to be constantly trained to stay up to date. It is about changes in the rules that the company has to pay for these costs.

Table.2. Compression of machine training

Security Selection Instructions	ETOS	BDFI	PPPD	PSOS	BDSA
100	56.42	67.48	84.19	79.87	94.02
200	54.79	65.74	82.61	78.45	92.73
300	54.31	63.40	80.41	77.19	91.72
400	53.02	62.59	78.78	75.20	90.83
500	50.91	60.30	77.64	72.73	90.46
600	49.42	58.37	75.44	71.29	88.82
700	47.61	56.64	74.29	69.57	88.45

Demand for compliance servers is estimated to be 20 percent higher. The servers store and manage an average of about 26 terabytes of data. This extra data storage by default includes all the hardware of the data center or cloud storage. An extra energy for cooling the data managers to maintain and exchange the data. Software is usually needed to help meet compliance requirements. This is necessary for checks to prove that your company complies with the rules.

Table.3. Compression of Costs

Security Selection Instructions	ETOS	BDFI	PPPD	PSOS	BDSA
100	66.31	63.38	84.03	78.86	96.02
200	64.82	61.41	81.61	76.66	94.03
300	64.02	60.28	81.20	75.86	92.83
400	61.69	59.07	79.60	75.19	92.35
500	60.68	58.70	77.28	73.76	90.92
600	60.04	57.17	76.03	72.67	89.76
700	59.38	56.67	73.30	72.19	88.99

Data protection costs continue to increase. Not only because prices are rising, but also because the current threats to data integrity are increasing. These threats require a multi-pronged approach. In addition to physical protection, the introduction of security software such as Antimalware and antivirus checkers. It requires firewalls, monitoring solutions on the network, security hardware at the user and user level. It includes security professionals who know how to handle all of this equipment.

Table.4. Compression of additional safety

Security Selection Instructions	ETOS	BDFI	PPPD	PSOS	BDSA
100	57.68	59.74	76.63	71.43	94.76
200	57.35	58.24	76.04	69.56	93.72
300	56.01	57.13	75.06	68.73	93.59
400	54.87	56.75	73.85	67.82	92.63
500	53.82	55.74	72.71	66.90	93.06
600	52.89	54.67	71.85	65.65	92.77
700	51.87	53.72	70.85	64.57	91.90

As data managers and security professionals take a lot of time to ensure that their processes and procedures are within the rules, there are also productivity implications for the company. If a particular need cannot be met at any time, there is a problem. We need to stop when an expert is working on problem solving. It is almost impossible to determine exactly how a company's productivity will be affected by compatibility.

Table.5. Compression of Data Security

Security Selection Instructions	ETOS	BDFI	PPPD	PSOS	BDSA
100	65.44	68.16	85.73	75.45	95.44
200	65.77	69.66	86.32	77.32	96.48
300	67.11	70.77	87.30	78.15	96.61
400	68.25	71.15	88.51	79.06	97.57
500	69.30	72.16	89.65	79.98	97.14
600	70.23	73.23	90.51	81.23	98.00
700	71.25	74.18	91.51	82.31	98.44

Every time a company develops a new technology or implements improvements within the company, we complicate the security process and therefore make it more expensive. The various activities are related to each other. They interact with each other so that the integrity of the data should always be reviewed. Compliance affects any business process, the infrastructure every time we use and use the product. The whole system has to deal with it.

Table.6. Compression of data integrity

Security Selection Instructions	ETOS	BDFI	PPPD	PSOS	BDSA
100	56.81	64.52	78.33	68.02	90.18
200	58.30	66.49	80.75	70.22	92.17
300	59.10	67.62	81.16	71.02	93.37
400	61.43	68.83	82.76	71.69	93.85
500	62.44	69.20	85.08	73.12	95.28
600	63.08	70.73	86.33	74.21	96.44
700	63.74	71.23	89.06	74.69	97.21

5. CONCLUSIONS

The Security architecture and security design are elements of how IT professionals work to provide comprehensive security for organizations. However, these two terms are slightly different. A security structure is a set of resources and components of a security system. Talking about the security structure is about how

a security system is set up and how all of its individual components function individually and collectively. For example, looking at a resource such as a network monitor or security software application in the context of an overall system can be described as referring to the security architecture. The Security design refers to the techniques and methods that facilitate the protection of those hardware and software components. Items such as handshaking and authentication may be part of the network security design. In contrast, applications, tools or resources that facilitate handshaking and authentication are part of the security framework.

REFERENCES

[1] Z. Jin, K. Yao, B. Lee, J. Cho and L. Zhang, Channel Status Learning for Cooperative Spectrum Sensing in EnergyRestricted Cognitive Radio Networks, *IEEE Access*, Vol. 7, pp. 64946-64954, 2019.

[2] A. Ali and W. Hamouda, Advances on Spectrum Sensing for Cognitive Radio Networks: Theory and Applications, *IEEE Communications Surveys and Tutorials*, Vol. 19, No. 2, pp. 1277-1304, 2016.

[3] M. El Tanab and W. Hamouda, Resource Allocation for Underlay Cognitive Radio Networks: A Survey, *IEEE Communications Surveys and Tutorials*, Vol. 19, No. 2, pp. 1249-1276, 2016.

[4] I. Kakalou, D. Papadopoulou, T. Xifilidis, K.E. Psannis, K. Siakavara and Y. Ishibashi, A Survey on Spectrum Sensing Algorithms for Cognitive Radio Networks, *Proceedings of International Conference on Modern Circuits and Systems Technologies*, pp. 1-4, 2018.

[5] Y. Wang, Z. Ye, P. Wan and J. Zhao, A Survey of Dynamic Spectrum Allocation based on Reinforcement Learning Algorithms in Cognitive Radio Networks, *Artificial Intelligence Review*, Vol. 51, No. 3, pp. 493-506, 2019.

[6] P. Yang, L. Li, J. Yin, H. Zhang and Z. Han, Dynamic Spectrum Access in Cognitive Radio Networks using Deep Reinforcement Learning and Evolutionary Game, *Proceedings of IEEE/CIC International Conference on Communications in China*, pp. 405-409, 2018.

[7] Y. Zhao, Z. Hong, Y. Luo, G. Wang and L. Pu, PredictionBased Spectrum Management in Cognitive Radio Networks, *IEEE Systems Journal*, Vol. 12, No. 4, pp. 3303-3314, 2017.

[8] A.M. Koushik, F. Hu and S. Kumar, Intelligent Spectrum Management based on Transfer Actor-Critic Learning for Rateless Transmissions in Cognitive Radio Networks, *IEEE Transactions on Mobile Computing*, Vol. 17, No. 5, pp. 1204-1215, 2017.

[9] X. Li, J. Chen, G. Zhao and M. Pietikainen, Remote Heart Rate Measurement from Face Videos under Realistic Situations, *Proceedings of IEEE International Conference on Computer Vision and Pattern Recognition*, pp. 4264-4271, 2014.

[10] R. Irani, K. Nasrollahi and T.B. Moeslund, Improved Pulse Dectection from Head Motions using DCT, *Proceedings of International Conference on Computer Vision Theory and Applications*, pp. 124-129, 2014.

[11] S. Thulasi Prasad and S. Varadarajan, Heart Rate Detection using Hilbert Transform, *International Journal of Research in Engineering and Technology*, Vol. 2, No. 8, pp. 12-18, 2013.