Secure Data-Encryption Strategy for Big-Data in Mobile Cloud

Sellam V, SVivek Reddy, K Praveen, G C Krishna, J Abhinay Rao

***Abstract:** Now-a-days data plays a key role in Information Technology and while coming to privacy of that data it has become a considerable issue to maintain data security at high level. Large amounts of data generated through devices are considered as a major obstacle and also tough to handle in real time scenarios. To meetwith consistent performance applications at present abandon encryptions techniquesbecausethe time for the execution and the completion of encryption techniques plays a key role during processing and transmissions of data. In this paper our moto is to secure data and proposed a new technique called Dynamic Data Encryption Strategy (DDES)which selectively encrypts data and uses some algorithms which provides a perfect encryption strategy for the data packages under some timing constraints. By this method we can achieve data privacy and security for big-data in mobile cloud-computing by using an encryption strategy respective to their requirements during execution time.*

***Keywords:** Big-data, Mobile Cloud Computing, Security, Encryption Strategy, Privacy.*

I. INTRODUCTION

In general, big-data represents high amount of data, more velocity and variety. Companies like Facebook, Google etc.., are using big data platform for storing and processing of data. With the evolution of internet, the world makes sure that people all are connected at the touch of a button and also technology is getting improved day-by-day in which people are more interested in using latest technology because it makes all works faster and smarter. Due to its more space and complexity, it becomes very complicated to handle big-data using current tools in real time. In this scenario, Cloud computing plays a key role in storing data in which it also allows the users to retrieve data from anywhere in the world by just one click. Cloud computing is an upcoming technology which is divided into various fields with a new aim that upcoming different new administrations are sent into the open, for example, parallel-processing. Mobile computing is the future of technology in which it allows the people to connect with internet and data that demands distribution.

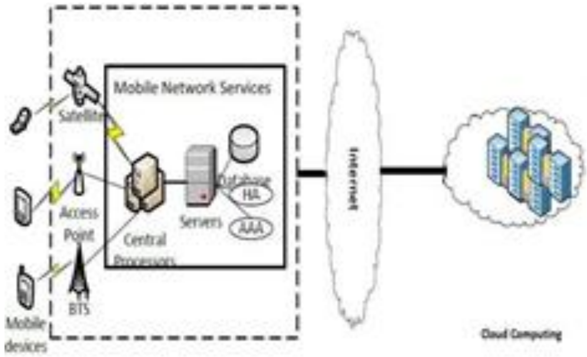


Figure 1: A representation of the connection between Cloud computing and the mobile users through internet.

Mobile Cloud computing refers to mobile users and cloud computing, which allows information sharing over multiple parties across different platforms. The information retrieval is a wireless communication between users in which they carry personal information through various channels, including social networking sites and other infrastructures. Including secure data management, data privacy, encryption, storage and transmissions as main aspects have been explored in some of the researches as follows. Though there are many useful benefits of mobile cloud computing, protecting data owners and user's privacy during the data retrieval process and also communications on social networks is the biggest problems due to un-encrypted data transmission.

In the above figure it is observed that there is no security or data privacy for the data which is transmitted to the cloud through internet. To overcome this issue we came up an encryption strategy which protects the data of both the users and owners. The proposed model for this process is called Dynamic Data Encryption Strategy Model (DDES).

II. RELATED WORK

Mobile Cloud computing refers to mobile users and cloud computing, which allows information sharing over multiple parties across different platforms. The information retrieval is a wireless communication between users in which they carry personal information through various channels, including social networking sites and other infrastructures. Including secure data management, data privacy, encryption, storage and transmissions as main aspects have been explored in some of the researches as follows.

Manuscript published on 30 October 2019.
***** Correspondence Author (s)

Mrs.V.Sellam, Assistant Professor, Computer Science and Engineering Department SRM Institute of Science and Technology, Chennai, India.

Mr.S.VivekReddy, Pursuing Bachelor of Technology, Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India.

Mr. K.Praveen, Pursuing Bachelor of Technology, Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India.

Mr.G.C.Krishna, Pursuing Bachelor of Technology, Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India.

Figure 2: Illustrating the Security issue of big data and cloud computing according to previous researches .

Existing System Privacy has turned into an impressive issue when the utilizations of enormous information are significantly developing in distributed manner. The advantages of these upcoming advances have improved the administration models and the other application exhibitions in different points of view. Be that as it may, the astoundingly developing volume of information sizes has additionally brought about numerous difficulties by and by. The time for the information encryption execution is one of the difficult problems which aimed the information preparation along with transmission. Numerous present products relinquish information security so as to achieve an assenting act level companioning with protection concerns. Regardless of numerous advantages of utilizing portable distributed computing, there are incredible worries in ensuring information proprietors' protection amid the correspondences on interpersonal organizations or versatile applications .One of the security concerns is brought about by decoded information transmissions because of the vast hand volume and continuous administration concerns. The usage of enormous information further prevents transmission from conveying figure writings.

The articulation "Tremendous Data" suggests the immense proportions of cutting edge information associations and governments assemble about individuals and our condition. The proportion of data made is required to twofold predictably, from 2500 exabytes in 2012 to 40,000 exabytes in 2020As Big Data stretches out through spouting cloud development, ordinary security instruments uniquely fitted to confirming little level, consistent data on the line and semi-withdrew frameworks are unique. For instance, examination for irregularity area will make an extreme number of peculiarities. In like manner, it is dim how to get back provenance in the current cloud establishments. Spilling demands in data ultra-responses times with security and insurance game plans.

III. ARCHITECTURE

The architecture of this project involves mobile users, cloud computing, wireless networks, privacy protection, data transmissions and clouds physical servers.

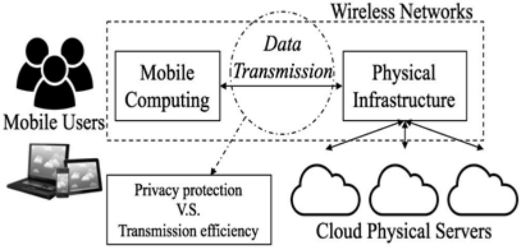


Figure 3: The architecture of cloud physical servers with respective to big data with data transmission andPrivacy protection.

A. *Mobile users and Mobile Computing*

These are the initial stages to generate data in which mobile users are responsible for large volumes of data in which mobile computing is the process where data is processed and stored in the cloud servers which also includes cloud computing.

B. *Data Transmission and Privacy protection*

Data transmission is the main process in the above architecture in which it transmits the data from mobile users to the physical cloud servers with great transmission efficiency. In order with the data transmission, data privacy is considered as an important issue so that privacy protection of the data packages must be completed before the data is going to be stores in the cloud physical servers. Here the privacy is maintained by introducing an encryption strategy for all the data packages present.

C. *Wireless Networks*

All these data transmissions and storing are done through wireless networks. Wireless networks are responsible for distributed data processing and transmission which allow the users to access their data from anywhere in the world.

IV.CONCEPTS AND PROPOSED SYSTEM

The architecture of this project involves mobile users, cloud computing, wireless networks, privacy protection, data transmissions and clouds physical servers.

They are:-

Phase I: Sorting by weights
Phase II: Data alternatives
Phase III: Output

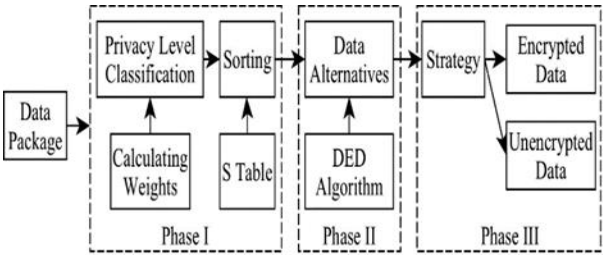


Figure 4: Representation of all 3 phases in DDES

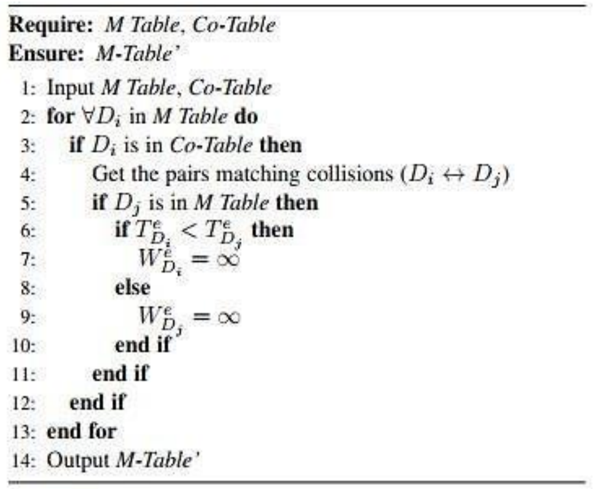
First phase in this approach is known as sorting by weight which is also known as planning phase of this technique. All the information sets will be composed at this stage which includes both security instances and execution time into account. In this phase the data packages are takes as input whereas the individual data package gets its own weight using privacy level classification. It uses weight simulation algorithm to calculate the weights and then they run privacy preserving sorting method. When sorting is executed, individual data packets achieve transformed weight and S Table is used to map all the sorted results into a table.

B. Data Alternative

The sorted results of S Table are accepted as input and we perform encryption strategy to the data packets with the highest weight value, where encryption should be performed under a specified timing constraint. Weights can be calculated by wm algorithm.Firstly we specify the timing constraint and the timing span to perform encryption then we apply Dynamically Regulate Encryption Algorithm. Where only the sensitive modified data is been encrypted, sensitive word is identified by which word has the highest weight value is considered as sensitive word to perform encryption.

C. Output

This phase, outlay the data which is been encrypted. The insensitive data is in unencrypted form and the sensitive data is encrypted there by securing the user data. The process aborts when all sensitive data is encrypted and when the data package doesn't contain any sensitive words to perform encryption. We view the sensitive modified data in the encrypted form. The output acquired is in encrypted form which indicatesthat the mobile users data is been secured which is the highest priority in our proposed work and it should be achieved in the specified timing constraint.



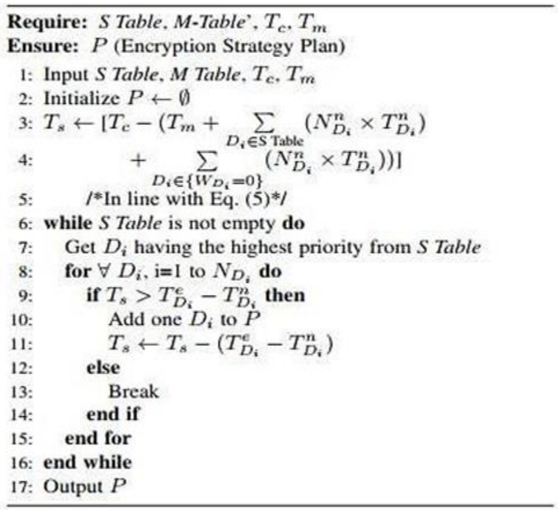
```
Require: M Table, Co-Table
Ensure: M-Table'
Input M Table, Co-Table
for $\forall D_i$ in M Table do
    if $D_i$ is in Co-Table then
        Get the pairs matching collisions $(D_i \leftrightarrow D_j)$
        if $D_j$ is in M Table then
            if $T^e_{D_i} < T^e_{D_j}$ then
                $W^e_{D_i} = \infty$
            else
                $W^e_{D_j} = \infty$
            end if
        end if
    end if
end for
Output M-Table'
```

V. ALGORITHMS

The main algorithms used in this project are Dynamic Encryption Determination algorithm (DED),Weight Modelization algorithm (WM) , S Table Generation algorithm (STG) .These algorithms are used to determine the best encryption technique with the available time.

At first the inputs are taken by reading weights of each data package individually by weight modelization algorithm and then DED algorithm calculates the best encryption strategy under some time constraints. The privacy level classification determines which type of data should have security of various level with respective of the input. Here time constraints plays key role in the process of data transmission and privacy protection with fastest transmission efficiency.

1.Dynamic Encryption Determination Algorithm **(DED):**DED algorithm is mainly used for calculations because it makes the security protection strategy by comparing the planning requirements and system requirement.



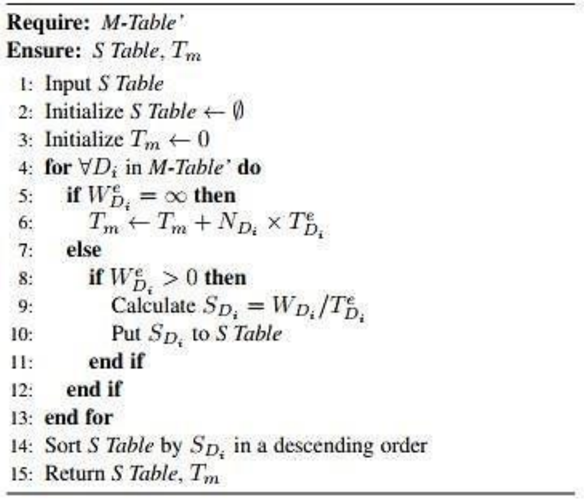
```
Require: S Table, M-Table', $T_c$, $T_m$
Ensure: P (Encryption Strategy Plan)
Input S Table, M Table, $T_c$, $T_m$
Initialize $P \leftarrow \emptyset$
$T_s \leftarrow [T_c - (T_m + \sum_{D_i \in \text{S Table}} (N^n_{D_i} \times T^n_{D_i})$
            $+ \sum_{D_i \in \{W_{D_i}=0\}} (N^n_{D_i} \times T^n_{D_i}))]$
        /*In line with Eq. (5)*/
while S Table is not empty do
    Get $D_i$ having the highest priority from S Table
    for $\forall$ $D_i$, i=1 to $N_{D_i}$ do
        if $T_s > T^e_{D_i} - T^n_{D_i}$ then
            Add one $D_i$ to P
            $T_s \leftarrow T_s - (T^e_{D_i} - T^n_{D_i})$
        else
            Break
        end if
    end for
end while
Output P
```

2. WeightModelization Algorithm (WM):

This algorithm is designed to support DED algorithm.S Table Generation algorithm (STG) .These algorithms are used to determine the best encryption technique with the available time

3. S Table Generation Algorithm:

This algorithm is designed to support DED algorithm.



```
Require: M-Table'
Ensure: S Table, $T_m$
Input S Table
Initialize S Table $\leftarrow \emptyset$
Initialize $T_m \leftarrow 0$
for $\forall D_i$ in M-Table' do
    if $W^e_{D_i} = \infty$ then
        $T_m \leftarrow T_m + N_{D_i} \times T^e_{D_i}$
    else
        if $W^e_{D_i} > 0$ then
            Calculate $S_{D_i} = W_{D_i} / T^e_{D_i}$
            Put $S_{D_i}$ to S Table
        end if
    end if
end for
Sort S Table by $S_{D_i}$ in a descending order
Return S Table, $T_m$
```

Therefore, all the above algorithms will ensure a perfect encryption strategy for their respective data packets under certain time constraints.

VI. CONCLUSION

This paper is solely based on the data security and privacy issues of big data which alsoincludes mobile cloud computing . In this proposed approach some algorithms are used to encrypt and decrypt data to maintain privacy of the customers and owners. The main algorithm was DED algorithm that was developed for encryption under different time constraints.

There a three phases in this proposed Dynamic Data Encryption Strategy Model in which the output from these phases determines the accurate encryption strategy for their respective data packets. Therefore, a perfect strategy ensures the privacy of the users.

ACKNOWLEDGEMENT

We would like to thank our project guide Mrs. Sellam V for helping us to find out the required resources in order to complete this project work in and also her key insights helped us to make the project efficient.

REFERENCES

1. S. Yu, G. Gu, A. Barnawi, S. Guo, and I. Stojmenovic. “Malware propagation in large-scale networks”-2015. IEEE Transactions on Knowl-edge and Data Engineering.
2. H. Liu, H. Ning, Y. Zhang, Q. Xiong, and L.“Yang.Role-dependent privacy preservation for secure V2G networks in the smart grid”-2104.IEEE Transactions on Information Forensics and Security.
3. Privacy-Preserving Public Auditing for Secure Cloud Storage Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, KuiRen, Member, IEEE, and Wenjing Lou, Member,IEEE.
4. Y. Li, W. Dai, Z. Ming, and M. Qiu. Privacy Protection for Preventing Data Over-Collection in Smart City. IEEE Transactions on Computers, 65:1339–1350, 2015.
5. S. Yu, W. Zhou, S. Guo, and M. Guo. A feasible IP traceback framework through dynamic deterministic packet marking. IEEE Transactions on Computers, 65(5):1418–1427, 2016.
6. S. Rho, A. Vasilakos, and W. Chen. Cyber physical systems technologies and applications. Future Generation Computer Systems, 56:436–437, 2016.
7. Sundaraguru R, and M.Banupriya, “Acknowledged Secure Data Dissemination” International Journal of Management, IT and Engineering, Vol.3, No.8, pp. 40-54, 2013.
8. Secure Certificateless Public Verification for Cloud-Based Cyber-Physical-Social Systems Against Malicious Auditors Yuan Zhang, Student Member, IEEE, ChunxiangXu, Member, IEEE, Shui Yu, Senior Member, IEEE, Hongwei Li, Member, IEEE, and Xiaojun Zhang.
9. G. Wu, H. Zhang, M. Qiu, Z. Ming, J. Li, and X. Qin.A decentralized approach for mining event correlations in distributed system monitoring Journal.
10. F. Tao, Y. Cheng, D. Xu, L. Zhang, and B. Li, “Cloud computing and internet of things- based cloud manufacturing service system.”,IEEE Transactions on Industrial Informatics, Vol no 10(2),pp 1435–1442,

AUTHORS PROFILE

Mrs.V.Sellam,M.E.,Assistant Professor, Computer Science and Engineering Department SRM Institute of Science and Technology, Chennai, India. Her main researches include data mining and data analytics, under her guidance many students published their projectjournal papers in Indexed journals and has been presented at International and National Conferences

Mr.S.VivekReddy is currently pursuing his Bachelor of Technology in Computer Science and Engineering at SRM Institute of Science and Technology, Chennai, India. He has professional experience in Database management systems and Web Development. Trained and certified in web development. His research interest includes Big-data analytics and related frameworks like Hadoop.He is technically skilled in front end and back end technologies.

Mr.K.Praveen is currently pursuing his Bachelor of Technology in Computer Science and Engineering at SRM Institute of Science and Technology, Chennai, India. He has professional experience in Application Development. His research work includes Security and Database Management. His skills include digital media marketing and he is also well known for social service.

Mr. G. C. Krishna is currently pursuing his Bachelor of Technology in Computer Science and Engineering at SRM Institute of Science and Technology, Chennai, India. His main research work emphasis on with module selection & programming and implementing them with proposed architecture of the system. He has exceptional skills in Management, Administration, Social media marketing and also technically skilled in networking and web development

Mr. J. Abhinay Rao is pursuing his Bachelor of technology in Computer Science and Engineering at SRM Institute of Science and Technology, Chennai, India. His main research work includes data science in which he also aims to complete his master’s degree. He is interested in technology and implementing engineering real time scenarios and society. He is technically skilled in DBMS and Python programming