OPEN ACCESS

Volume: 11

Special Issue: 1

Month: July

Year: 2023

E-ISSN: 2582-0397

P-ISSN: 2321-788X

Impact Factor: 3.025

Received: 08.05.2023

Accepted:13.06.2023

Published: 01.07.2023

Citation:
Kumbhar, Shreedhar Maruti, and B. Nisarga. "Big Data Privacy-Preserving Data Encryption Strategy in Mobile Cloud Computing." *Shanlax International Journal of Arts, Science and Humanities*, vol. 11, no. S1, 2023, pp. 142–48.

DOI:
https://doi.org/10.34293/sijash.v11iS1-July.6329

Big Data Privacy-Preserving Data Encryption Strategy in Mobile Cloud Computing

Shreedhar Maruti Kumbhar
Department of Computer Applications
Raja Rajeswari College of Engineering

Nisarga B
Department of Computer Applications
Raja Rajeswari College of Engineering

Abstract

When it comes to large data applications in cloud computing, privacy has become a significant concern. The advantages of implementing these developing technologies have enhanced or modified service models and boosted application performancein several ways. However, the exponential growth in data volumes has brought forth a host of practical problems. The processing time required for data encryption is one of the major difficulties encountered in data processing and transmission. Many current applications forsake data passwords in order to maintain acceptable speed while yet taking privacy concerns into account. In this study, our main concern is privacy. and offer a unique data encryption technique dubbed Dynamic Data Encryption Strategy (D2ES).Under time restrictions, we propose to selectively encrypt data and apply privacy categorization algorithms. This method is intended to maximise the privacy protection scope by employing a selective encryption strategy within the execution time constraints. In our trials, the effectiveness of D2ES was examined, providing verification of the privacy increase.

Keywords: Privacy-Preserving, Data Encryption Strategy, Big Data, Mobile Cloud Computing, Cybersecurity.

Introduction

In recent years, the development of portable cloud computing technologies has made several applications possible. in people's lives. Involving humans in cloud computing and wireless connection loops provides an alternate method of retrieving information derived from watching humans' behaviours and interactivities across numerous social networks and mobile apps. Further more Cloud computing is a new technology that has grown into innumerable industries, resulting in the introduction of many new service deployments to the public, such as cellular parallel computing and distributed scalable data storage. Big data penetrations have further enhanced the channels for obtaining information from the vast number of data generated by mobile apps across numerous platforms, domains, and systems. Big data has become a widely used technology that is used in many different industrial industries.

Considering the many advantages of employing mobile cloud computing, there are significant issues about preserving data owners' privacy while communicating on social networks or mobile apps. Due to the high volume of data, one of the privacy problems is generated by unencrypted data transmissions. Many people consider an acceptable level of performance to be with online information promotions, moving, applications no longer use cypher texts. This phenomena may result in the disclosure of personal information difficulties because plain texts make it easy for adversaries to collect information in a number of methods, including jamming, monitoring, and spoofing [15]. This privacy problem is significant because it involves a conflict between security levels and performance, which is typically associated with time restrictions. demonstrates the high-level architecture of mobile cloud with examples of handling privacy measures. The critical issue is that, due to workload volume and real-time service considerations, most modern wireless transfers transmit plain-texts. The use of large data prevents transmission from carrying cipher-texts. The broken-line box in the illustration represents the target protection location, indicating that data flows between physical infrastructure include computing on the go in the mobile cloud must be safeguarded. D2ES employs two key techniques: (1) categorising data packages according to their privacy level, and (2) determining if data packages can be encrypted within the time restrictions.

Literature Survey

According to wanlei zhou, they discovered a factor in which only a restricted number of computers and routers are participating in an attack session. As a result, rather than labelling every node on the Internet as present techniques do, we simply need to flag specific involved nodes for traceback purposes. Based on this discovery, we offer a unique MOD traceback approach based on the DPM process. To traceback to the implicated attack source, we must label these involved ingress routers using the usual DPM approach. We require participating a traffic routers should be installed monitor, similar to previous methods.

In the words of Emryas A Felke, a Cyber-Physical System (CPS) is a new digital system generation that emphasises the complex integration as well as interdependencies between cyberspace (digital world) and the physical world. The CPSs are made up of highly integrated physical and computational parts, as well as control and communication aspects. Because it is a cutting-edge technology, it has applications in healthcare, academia, government, organisation, robotics, and other fields. Many academics have completed their studies in these areas.However, there are few literatures or surveys on CPS applications and security issues. This study does an investigational survey on the security and applicability of CPS in many areas from 2012 to 2018.
Furthermore, vulnerability identification is a key part in preventing privacy leaks. Mulliner et al. developed a detective technique focused on the vulnerabilities induced by Graphical User Interface (GUI) element abuse. This technique addressed the misuses of GUI element characteristics in a GUI-based application environment. An efficient privacy policy compliance verification approach is crucial in the setting of huge data. constructing a safe searching system. Because opponents are not monitored in most current operating environments, the lack of tracking capability in Web browsers might lead to privacy problems. A well-designed secure networking architecture can also slow the pace of threat amplification [30].

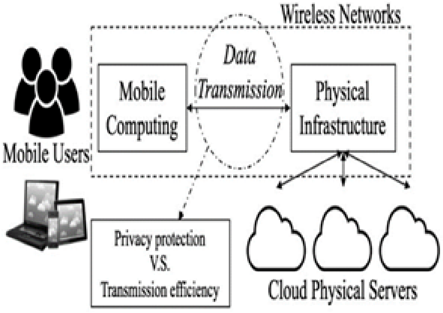


Figure 1 High Level Architecture of Mobile Cloud Computing Illustrating the Balance between Privacy Protection and Transmission Efficiency

Existing System

This study is an extension of our previous research and work on the broad data encryption approach of large data in cloud systems. In comparison to our previous work, the critical added value of this study is to increase the implementation adaptation of the suggested technique by further strengthening the mechanism’s features. Our earlier work [16] primarily represents the dynamic data encryption strategy’s operational concept and the implementation technique. In this study, we expanded on our previous work by improving the mechanism design for each mode phase. Paired Data and Pairs Matching Collision are two critical words for performing the data encryption approach. Furthermore, ensuring effective wireless communications is critical in a high performance mobile cloud system in terms of user controllability. One study addressed the issue by establishing two-dimensional paired connections over the Radio Waves for Electronics in Daily Life (FR4CE) for both appliances and controllers while consumers attempted to connect with appliances. Another study looked at user-machine interaction concerns from a different angle. According to the study, the important element of safeguarding privacy is building a successful method that emphasises both human engagement and system controls. To effectively forecast opponents, both sides must be matched and merged.

Despite the many benefits of using the mobile cloud, there are serious concerns about protecting data owner’ privacy while using social media or mobile applications for communication. Unencrypted data transfers are one of the privacy issues brought on by the large volume of data. In order to transport mobile cloud data at a reasonable pace, several apps forgo the usage of cypher messages. Given that plain texts make it simple for adversaries to get information in a number of ways, this phenomenon might cause privacy issues. methods, including jamming, monitoring, and spoofing. This privacy problem is significant because it involves a conflict between security levels and performance, which is typically associated with time restrictions.

Another issue is that opponents do not provide any identity information, making it difficult to produce danger warnings. Following that, the data analysis approach is regarded a promising solution to identify trustworthy data when the data size grows huge, as addressed by previous study. Nonetheless, these studies primarily focus on danger identification through the use of a range of analytic methodologies. Our study presents a method for increasing the pace of encrypted data while taking the value of data encryptions into account.

Notwithstanding the fact that several access control techniques have been developed, there are some weaknesses.. Data transfers in wireless networks provide several chances for attackers to infiltrate connections and take data. Privacy may be jeopardised if any data segments are obtained by enemies using powerful data mining techniques. In this research, we propose a unique method for selectively encrypting data in order to ensure privacy even during data transmission. Data encryptions are based on the return value of the encryptions and data characteristics to reduce the possibility of privacy leaks when attackers use data mining techniques.

Proposed System

This study discusses the conflict between data transmission efficiency and security. To address the issue, we present a unique method for selectively encrypting data in order to maximise the volume of encrypted data while adhering to the requisite scheduling limitations. The suggested model is known as the Dynamic Data Encryption Strategy (D2ES) concept, and it is intended to secure data owners' privacy to the greatest extent possible when employing the appropriate devices and networking infrastructure. Figure 1 depicts the high level architecture of mobile cloud with examples of addressing privacy safeguards. The critical issue is that, due to workload volume and real-time service considerations, most modern wireless transfers transmit plain-texts.

The use of large data prevents transmission from carrying cipher-texts. The broken-line box in the illustration represents the target protection location, indicating that data flows between physical infrastructure and mobile processing in the mobile cloud must be safeguarded. D2ES employs two key techniques: (1) categorising data packages considering their privacy level, and (2) determining if data packages can be encrypted within the time restrictions. We create and present the Dynamic Encryption Determination (DED) method, which determines data encryption options based on scheduling restrictions and facility capabilities.

Furthermore, to increase privacy protection, we offer a Pairs Matching Collision (PMC) approach. This method is intended to avoid the situation in which two plain messages might compromise users' privacy even if leaking each simple text is not dangerous. The PMC mechanism's operational premise is to ensure that at least one of two pre-defined pair data is encrypted. When communicated or operated in plain text, the associated data must include privacy information.

The definition of paired data is provided

This is the critical phase for picking data packages for encryption procedures. To complete this step, we propose the DED algorithm. S Table will be utilised as a reference for protection efficiency. The working premise is that data packages with higher SDi values have greater level alternative priority than data packages with lower SDi values. Selecting data packages consists of several sub-steps.

First, a time scope must be determined. Tc is the provided temporal restriction. As a result, the temporal scope is [0, Ts], with the value of Ts obtained from Eq. (1).

Ts = Tc X s(i) = 0 (NDi T n Di) (1)

Following that, data alternatives are carried out. The execution time of each encrypted data packet is T e Di . We begin by encrypting the data packet with the greatest SDi value possible. The procedure will continue until two requirements are satisfied. All of the data units are encrypted in the first scenario. The second scenario is when the actual time T e Di is longer than the remaining time.

This stage primarily produced an encryption plan according to the outcomes of Phase II. Under certain conditions, material with a higher degree of encryption priority will be chosen for encryption. The rest of The information won't be encrypted, therefore plain text operations will be used. Section 4 shows a motivational example to offer a more simple overview. The goal is to determine the method that will generate the most total PWV by selecting a group of data packages for encryptions. The retrieval of PWVs is dependent on data protection methods. The basic premise is that a higher level of data encryption complexity earns a higher PWV. Table 1 displays a mapping of data package kinds and their values. This table is known as the M Table. D1, for example, includes three data packages that need 5-unit time for encryption and 1-unit time for non-encryption.

D1 has a greater privacy weight value of 2.5 than any other kind. The WM algorithm was created to change the M Table using weight values. When evaluating the relationships between packages, the goal of this technique is to determine if a data package is a must-encrypted objective. As a result, the pairings matching collisions are used in this approach to recognise paired data . An M Table and a Co-Table are used as inputs. This procedure produces a modified M Table, which is denoted as an M-Table'. MTable' serves as an input to both Algorithms.Furthermore, a Co-Table is a table that maps all paired data and is pre-defined by security standards or developers.

Results

In this part, we exhibited a few experimental findings that showed the disparities in predicted execution time.

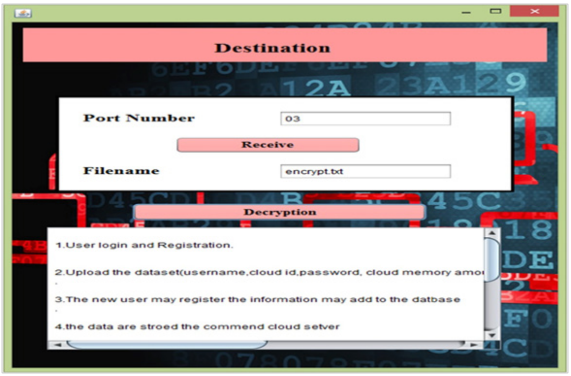
Figure 1 and Figure 2 depicted the outcomes of the same experiment rounds.

The majority of P values achieved with D2ES were close to the ideal results obtained by the BF method. Under Setting, the duration between D2ES and ideal solutions reflected a near performance between D2ES and optimal solutions in getting the whole privacy weight. Demonstrated our technique required a shorter execution time than BF, which agreed with the experiment's rounds. The rationale for the faster execution time was that our technique could obtain a lower P value than the best solutions. A lower level P value may bring about faster execution time.

Actual calculation time distributions of the proposed D2ES, dynamic programming, and BF algorithms in the Setting 1 context were compared. The computation time was shown via the vertical axis.Microseconds are employed as a measure time. The computation rounds were indicated by the horizontal axis. To make the distribution trends more clear, the data were sorted by the duration of the calculation time. The identical figure arrangement was used for

As shown in the pictures, our suggested technique outperformed both dynamic programming and BF algorithms. All test data could be calculated in an appropriate polynomial time.

In summary, our D2ES performed better in many testing conditions. The experimental results met our design aim and were consistent with the theoretical conclusions. Future study will focus on practical metrics in real-world assessments.



Destination

Port Number: 03

Filename: encrypt.txt

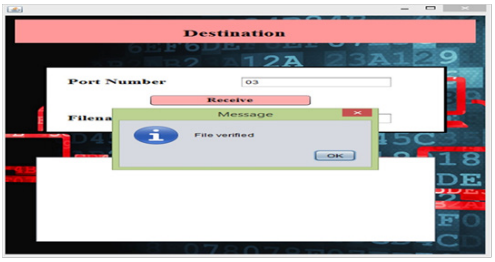
1.User login and Registration.

2.Upload the dataset(username,cloud id,password, cloud memory amo

3.The new user may register the information may add to the datbase

4.the data are stroed the commend cloud setver

Figure 2 Experiment Rounds



Port Number: 03

File verified

Figure 3 File Verification

Conclusions

This article focused on huge data privacy challenges and practical applications in cloud technology. The proposed approach, D2ES, was developed to maximise the efficacy of privacy measures. The primary technique behind the D2ES paradigm was the DED approach, which was developed to offer alternative data packets for passwords under various scheduling constraints. The results of the experimental assessments showed that the suggested technique performed superiorly and adaptively.

References

1. 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.
2. S. Yuu, Gg. Guu, A. Barntawi, I. Stojmenovic and S. Guo. spread of malware on gigantic networks. 2015, 27(1):170-179 of the Transactions of the IEEE on Learning and Data Engineering, vol.
3. S. Liu, Qq. Qun, L. Chen, and L. Nei. SMC: A useful framework for exchanging data via dispersed data streams while protecting privacy. 2015, 1(2):68–81 The Annals Transactions on Big Data.
4. S. Rhou, A. Vasrilakos, and W. Chgen. Uses and technology for cyber-physical systems. 56:436–437, Current Gen Information Systems, 2016.
5. L. Wut, K. Wju, A. Sirm, M. Chuwerchill, J. Choi, A. S. Klasky, C. Huang, and Stathopoulos. Blob-filaments in fusion plasma: towards spatial characteristic tracking and immediate detection. 2016; 2(3), Proceedings of the IEEE on Big Data.
6. S. Mahyarjan, Q. Zhfu, Y. Zhang, S. T. Basar and Gjessing. A Stackelberg game technique for sustainable management of demand response in the smart electricity system. 2013;4(1):120–132;IEEE Journal on Smart Grid.
7. M. Qfdiu, M. Zhotng, J. Li, K. Gai, and Z. Zodng. Green clouds phase-change memory optimization via the genetic algorithm. 2015, Transactions of the IEEE on Computers, 64(12), 3528–3554.
8. H. Lieu, H. Niyhng, Y. Zhayng, Q. Xiorng, and L. Yatng. Privacy protection for secure V2G networking in the smart grid based on a user's role. 2014; 9(2):208-220 in IEEE Transactions on Communication Forensics and Protection.
9. F. Taofth, Y. Chefng, D. Xru, L. Zharng, and B. Li. CCIorjT-CMhfg: cloud manufacturing service solution powered by the internet of things and cloud computing. 2014;10(2):1435–1442 in the IEEE Trans on Industrial Informatics.
10. 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 of parallel and Distributed Computing, 73(3):330–340, 2013.
11. S. Yu, W. Zhou, R. Doss, and W. Jia. Traceback of DDoS attacks using entropy variations.

IEEE Transactions on Parallel and Distributed Systems, 22(3):412–425, 2011. [12] 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.

12. S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang. Discriminating DDoS attacks from flash crowds using flow correlation coefficient. IEEE Transactions on Parallel and Distributed Systems, 23(6):1073– 1080, 2012.