World Applied Sciences Journal 29 (Computer Sciences, Engineering and Its Applications): 115-120, 2014
ISSN 1818-4952
© IDOSI Publications, 2014
DOI: 10.5829/idosi.wasj.2014.29.csea.2228

Concealed Information *Aggregation theme for Multiple applications in Wireless Device Networks*

R. Udayakumar, K.P. Kaliyamurthie, Khanaa and A.V. Allin Geo

School of Computing Science, Bharath University, Chennai-73, India

Abstract: Security challenges area unit still amongst the most important obstacles once considering the adoption of cloud services. This triggered plenty of analysis activities, leading to a amount of proposals targeting the varied cloud security threats aboard with these security problems the cloud paradigm comes with a replacement set of distinctive options that open the trail towards novel security approaches, techniques and architectures. This paper provides a survey on the doable security deserves by creating use of multiple distinct clouds at the same time. varied distinct architectures area unit introduced and mentioned in line with their security and privacy capabilities and prospects.

Key words: Cloud · Security · Privacy · Multi-Cloud · Application Partitioning · Tier Partitioning · Data Partitioning · Multi-party Computation

INTRODUCTION

Cloud computing offers dynamically scalable resources provisioned as a service over the net. The third party, on-demand, self-service, pay-per-use and seamlessly scalable computing resources and services offered by the cloud paradigm promise to scale back capital as well as operational expenditures for hardware and software. Clouds can be categorized taking the physical location from the perspective of the user into account [1]. A *Public Cloud* is offered by third-party service providers and involves resources outside the user's premises. In case the cloud system is installed on the user's premise usually in the own data center this setup is called *Private Cloud*. A hybrid approach is denoted as Hybrid Cloud. This paper can think about public clouds, since these services demand for the highest security requirements but also as this paper will start arguing includes high potential for security prospects. In public clouds, all of the 3 common cloud service layers (IaaS, Paas, SaaS) share the commonality that the end-users' digital assets are taken from an intra organizational to an inter-organizational context. This creates a number of problems, amongst that security aspects are considered the foremost crucial factors once considering cloud computing adoption [2]. Legislation and compliance frameworks raise further challenges on the outsourcing of data, applications and processes. The high privacy standards within the EU, e.g.,and their legal variations between the continent's countries give rise to specific technical and structure challenges [3]. One plan on reducing the chance for data and applications in a public cloud is the simultaneous usage of multiple clouds. Many approaches using this paradigm are projected recently. They dissent in partitioning and distribution patterns, technologies, cryptographic strategies and targeted situations additionally as security levels. This paper is Associate in Nursing extension of [4] and contains a survey on these completely different security by multi-cloud adoption approaches. It provides four distinct models in type of abstracted multi-cloud architectures. These developed multi-cloud architectures allow to categorize the available schemes and to analyze them according to their security benefits. An assessment of the different methods with regards to legal aspects and compliance implications is given in particular Sensor networks promise viable solutions to several observation issues. However, the sensible preparation of sensing element networks faces several challenges obligatory by real-world demands. sensing element nodes usually have restricted computation and communication resources and battery

Corresponding Author: R. Udayakumar, School of Computing Science, Bharath University, Chennai-73, India.

power. Moreover, in several applications sensors are deployed in open environments and thence are susceptible to physical attacks, doubtless compromising the sensor's cryptologic keys. one among the essential and indispensable functionalities of sensing element networks is that the ability to answer queries over the information non inheritable by the sensing element. [5] k-anonymity notion is adopted to be used in wireless networks(WSN) as a security framework with two levels of privacy.A base level of privacy is provided for the data shared with semi trusted and a deeper level of privacy is provided against eavesdroppers method, some portions of data are encrypted and the rest is generalized generalization shortens the size of the information transmitted within the network inflicting energy saving energy. In our system, this trade-off is showing intelligence managed by a system parameter, that adjusts the number of information parts to be encrypted. We use a technique supported bottom up clump that chooses the information parts to be encrypted among the ones that causes maximum information loss when generalized.In this way, a high degree of energy saving is realized within the limits of information loss. Our analysis show that the proposed method achieves the desired privacy levels with low information loss and with considerable energy saving.

The planned theme has 3 contributions. First, it's designed for a multi application surroundings. the bottom station extracts application-specific information from aggregate cipher texts. Next, it mitigates the impact of compromising attacks in single application environments. Finally, it degrades the harm from unauthorized aggregations. To prove the proposed scheme's strength and potency, we tend to conjointly conducted the excellent analyses and comparisons within the finish.

A wireless sensing element network, information aggregation theme that reduces an oversized quantity of transmission is that the most sensible technique.

Related Works:

"SIA: Secure Information Aggregation in Sensor Networks"
Author : Bartosz Przydatek, Dawn Song, Adrian Perrig in the year 2003

In our framework bound nodes within the sensing element network, known as aggregators, facilitate aggregating info requested by a question, that considerably reduces the communication overhead.

By constructing economical sampling mechanisms and interactive proofs, we have a tendency to change the user to verify that the solution given by the individual may be a sensible approximation of truth worth even once the individual and a fraction of the sensing element nodes area unit corrupted [8]. In explicit, we have a tendency to gift economical protocols for secure computation of the median and therefore the average of the measurements, for the estimation of the network size and for locating the minimum and most sensing element reading.

"Security in Wireless Sensor Networks: Issues and Challenges"
Author: Al-Sakib Khan Pathan, Hyung-Woo Lee in the year2004

Wireless device Network is AN rising technology that shows nice promise for varied artistic movement applications each for mass public and military.

The sensing technology combined with process power and wireless communication makes it remunerative for being exploited in abundance in future.

The intent of this paper is to analyze the safety connected problems and challenges in wireless device networks. we tend to establish the safety threats, review planned security mechanisms for wireless device networks.

"Secure Aggregation for Wireless Networks"
Author: Lingxuan Hu David Evans in the year 2007

An rising category of necessary applications uses unexpected wireless networks of low-power detector devices to observe and send info a couple of probably hostile setting to a strong base station connected to a wired network.

To conserve power, intermediate network nodes ought to combination results from individual sensors.

We gift a protocol that has a secure aggregation mechanism for wireless networks that's resilient to each interloper devices and single device key compromises.

CDAMA: CDAMA is meant by mistreatment multiple points, every of that has totally different order. area unit able to}acquire one scalar of the particular purpose through removing the results of remaining points the protection of CDAMA and BGN are supported the hardness assumption of subgroup call downside, whereas CDAMA needs a lot of precise secure analysis for parameter choices, discussing in Section six.2. we have a tendency to use CDAMA (k ¼ 2) to clarify however it works in multiple teams.

Aggregation with Secure Counting: The main weakness of uneven CDA schemes is that associate degree noble metal will manipulate mass results while not encoding capability. associate degree noble metal is in a position to extend the worth of mass result by aggregating the same cipher text of sensed reading repeatedly, or decrease the value by selective aggregation. Since the BS does not know the exact number of cipher texts aggregated (here, we call "count"), repeated or selective aggregation may happen. To avoid this problem, we adopt CDAMA (k ¼ 2) scheme to provide secure counting for single application case, i.e., the BS exactly knows how many sensed readings are aggregated while it receives the final result [6].

Despite of all the plug close the cloud, customers square measure still reluctant to deploy their business within the cloud. Security problems in cloud computing has compete a significant role in swiftness down its acceptance, in truth security hierarchal initial because the greatest challenge issue of cloud computing security might improve attributable to centralization of knowledge and raised security-focused resources. [7] On the opposite hand issues persist concerning loss of management over bound sensitive information and also the lack of security for hold on kernels entrusted to cloud suppliers. If those suppliers haven't done smart jobs securing their own environments, the customers can be in bother. measurement the standard of cloud suppliers' approach to security is troublesome as a result of several cloud providers won't expose their infrastructure to customers.

We propose a completely unique framework for secure data aggregation in massive device networks. In our framework certain nodes in the sensor network, called aggregators, help aggregating information requested by a query, which substantially reduces the communication overhead. By constructing economical sampling mechanisms and interactive proofs, we tend to change the user to verify that the solution given by the individual may be a smart approximation of truth price even once the individual and a fraction of the device nodes square measure corrupted. especially, we present efficient protocols for secure computation of the median and the average of the measurements, for the estimation of the network size and for finding the minimum and maximum sensor reading. Our protocols require only sub linear communication between the aggregator and also the user. To the simplest of our information, this paper is that the initial on secure info aggregation in device networks that may handle a malicious someone and sensor nodes.

Wireless sensing element Network (WSN) is associate rising technology that shows nice promise for numerous futurist applications each for mass public and military. The sensing technology combined with process power and wireless communication makes it moneymaking for being exploited in abundance in future. The inclusion of wireless communication technology conjointly incurs numerous styles of security threats. The intent of this paper is to analyze the safety connected problems and challenges in wireless sensing element networks. we have a tendency to establish the safety threats, review planned security mechanisms for wireless sensing element networks. we have a tendency to conjointly discuss the holistic read of security for making certain bedded and sturdy security in wireless sensing element networks.

System Architecture: Admin collect all type of sensor data to be collected together first. Next, it will aggregate related data together. This process done by cluster head. Cluster Head monitor each and every step. After finish, the clustering process It will forward to base station. The base station validates the user by using the generated code after that it will be accessible. The valid user only visible that information. The base station count the number of messages also. It is used for multiple application also.

Project Statement: Data aggregation theme that reduces an outsized quantity of transmission is that the most sensible technique. In previous studies, homomorphic encryptions are applied to hide communication throughout aggregation specifiedenciphered knowledge will be aggregate algebraically while not secret writing. Since aggregators collect knowledge while not secret writing, adversaries don't seem to be able to forge aggregate results by compromising them. However, these schemes don't seem to be satisfy multi-application environments. Second, these schemes become insecure just in case some detector nodes are compromised. Third, these schemes don't offer secure counting; so, they'll suffer unauthorized aggregation attacks. Therefore, we tend to propose a brand new hid knowledge aggregation theme extended from Boneh et al.'s homomorphic public encoding system. The projected theme has 3 contributions.

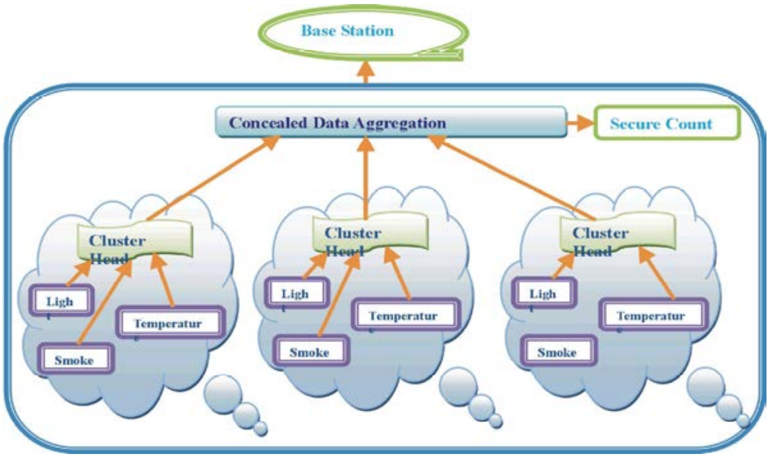


Fig 1:

Implementation: In our Project we use Front End as JAVA and Back End as a MYSQL 5.5.

JDK 1.6: In our project we are using java to design the application process. Java contains swing packages that are used to design the view page easily. Since java is an open source and platform independent this makes the application more flexible.

MYSQL 5.5: MYSQL 5.5 may be a electronic information service management system developed by Microsoft. As a information, it's a wares whose primary operate is to store and retrieve knowledge as requested by alternative software system applications, be it those on a similar laptop or those running on another laptop across a network (including the Internet). There area unit completely different workloads (ranging from tiny applications that store and retrieve knowledge on a similar laptop, to voluminous users and computers that access Brobdingnagian amounts of knowledge from the net at a similar time).

Definition:

- Collections:
- JSP
- Servlet
- Thread
- MYSQL

JSP: In our project we tend to are victimization JSP to style the appliance method. Java Server Pages (JSP) may be a server-side programming technology that permits the creation of dynamic, platform independent methodology for building Web-based applications. JSP have access to the whole family of Java APIs, together with the JDBC API to access enterprise databases.

Servlet: In our project we are using servlet to control the application process. Servlets are modules that run within the server and receive and respond to the requests made by the client.

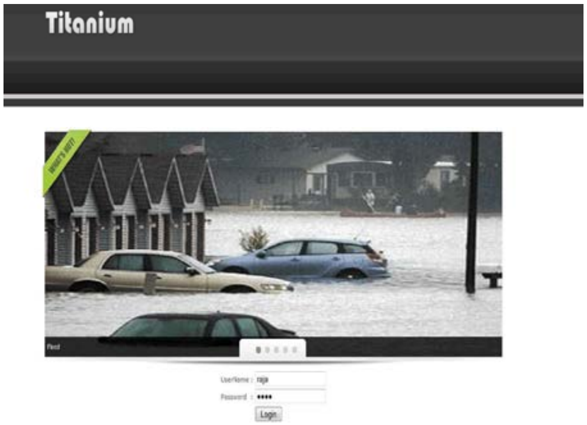
Servlet retrieve most of the parameters using the input stream and send their responses using an output stream. Servlets provide a component-based, platform-independent method for building Web-based applications, without the performance limitations of CGI programs. Servlets have access to the entire family of Java APIs, including the JDBC API to access enterprise databases.

Collections: The Java Collections API's provide Java developers with a set of classes and interfaces that makes it easier to handle collections of objects. In a sense Collection's works a bit like arrays, except their size can change dynamically and they have more advanced behavior than arrays. In this project we are using Array List, Map and Set for saving values and do some function using that values.

In the future, we wish to apply CDAMA to realize aggregation query in Database-As-a-Service (DAS) model. In our project we have a tendency to tend to are mistreatment JSP to vogue the appliance methodology. Java Server Pages (JSP) could also be a server-side programming technology that allows the creation of dynamic, platform independent methodology for building Web-based applications. JSP have access to the full family of Java APIs, along side the JDBC API to access enterprise databases. A client in DAS model is harder than compromising a sensor). Those drawbacks will no longer be issues in CDAMA.

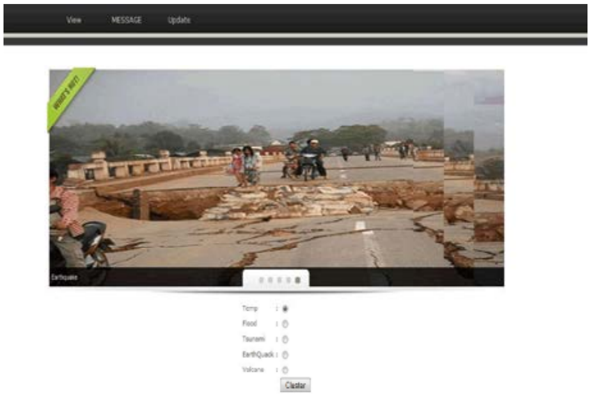
Result and Screen Shots:

User Interface Design:



UserName : raja
Password : ••••
Login

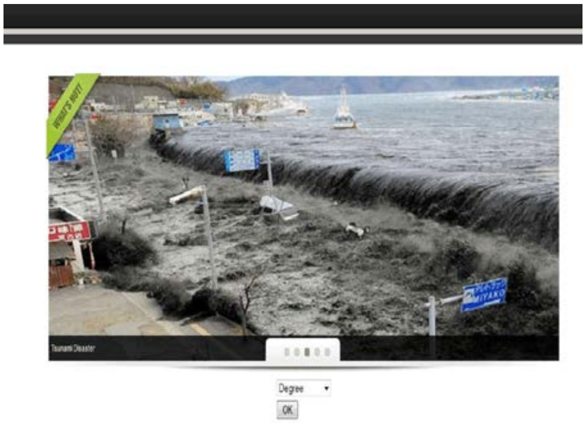
Fig 2:



Temp : ●
Flood : ○
Tsunami : ○
EarthQuack : ○
Volcano : ○
Clustar

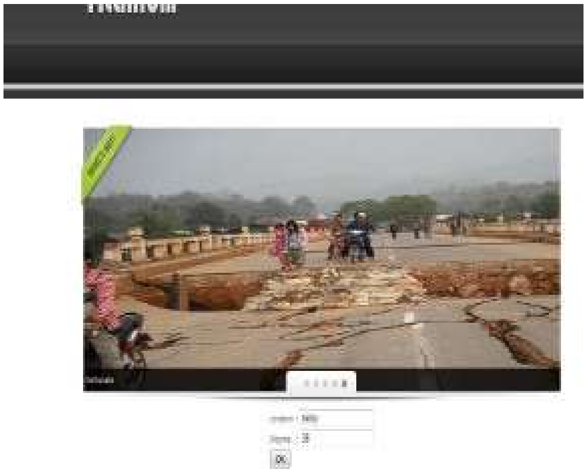
Fig 3:

Preprocessing:



Degree ▾
OK

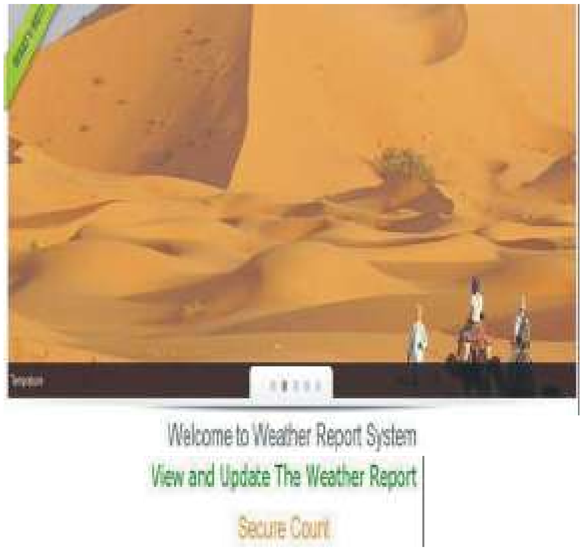
Fig 4:



OK

Fig 5:

Concealed Data Aggregation



Welcome to Weather Report System
View and Update The Weather Report
Secure Count

Fig 6:

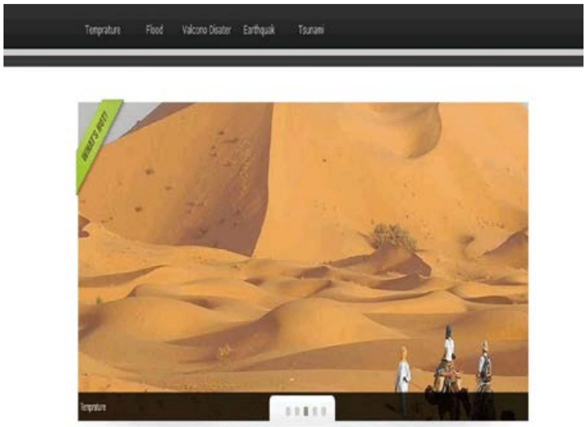


Fig 7:

CONCLUSION

Multi-application environment, CDAMA is that the initial CDA theme. Through CDAMA, the cipher texts from distinct applications are often aggregate, however not mixed. For one application atmosphere, CDAMA continues to be safer than alternative CDA schemes. Once compromising attacks occur in WSNs, CDAMA mitigates the impact and reduces the injury to an appropriate condition. Besides the higher than applications, CDAMA is that the initial CDA theme that supports secure reckoning. Finally, the performance analysis shows that CDAMA is applicable on WSNs whereas the quantity of teams or applications isn't massive.

AXCKNOWLEDGMENT

The Author would like to thank the staff members guided to finish the Paper and the researchers encouraged to reveal the Paper. And Sincere thanks to the reviewers to this paper and their welcome suggestions.

REFERENCES

1. Security and Privacy Enhancing Multi-Cloud Architectures Ieee Transactions on Dependable and Secure Computing Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono and Ninja Marnau on 2013.
2. Gens, F., 0000. “IT Cloud Services User Survey, pt.2: Top Benefits & Challenges,” Blog post on IDC Survey, 2008. [Online]. Available: http://blogs.idc.com/ie/?p=210
3. Malinverno, P., 2012. “Cloud computing in europe,” Gartner Application Architecture, Development & Integration Summit, June 2012. [Online]. Available: http://www.gartner.com/it/page.JSP?id= 2032215
4. Bohli, J.M., M. Jensen, N. Gruschka, J. Schwenk and L.L. Iacono, 2011. “Security prospects through cloud computing by adopting multiple clouds,” in 4th IEEE International Conference on Cloud Computing (CLOUD). IEEE.
5. k-anonymity Based Privacy Preerving for Data Collection in Wireless Sensor Networks k.p. kaliyamurthie, D. Parameswari and R.Udyakumar june 2013 [Online], Avalable :http://www.indjst.org/vol6(58)
6. Wu, Y., 2004. “Classify Encrypted Data in Wireless Sensor Networks,” Proc. IEEE 60th Vehicular Technology Conf., pp: 3236-3239.
7. Westhoff, D., J. Girao and M. Acharya, 2006. “Concealed Data Aggregation for Reverse Multicast Traffic in detector Networks: coding, Key Distribution and Routing Adaptation, ”IEEE Trans. Mobile Computing, 5(10): 1417-1431.
8. Girao, J. and G. Heidelberg, 2005. “CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks,”.