A new Security Mechanism for Vehicular Cloud Computing Using Fog Computing System

Mhidi Bousselham
Ibn Tofail University
ENSA Kenitra, Morocco
mhidi.bousselham@uit.ac.ma

Nabil Benamar
The Graduate School of Technology
Moulay Ismail
University Meknes, Morocco
n.benamar@est.umi.ac.ma

Adnane Addaim
Ibn Tofail University
ENSA Kenitra, Morocco
adnane.addaim@uit.ac.ma

***Abstract*—Recently Vehicular Cloud Computing (VCC) has become an attractive solution that support vehicle's computing and storing service requests. This computing paradigm insures a reduced energy consumption and low traffic congestion. Additionally, VCC has emerged as a promising technology that provides a virtual platform for processing data using vehicles as infrastructures or centralized data servers. However, vehicles are deployed in open environments where they are vulnerable to various types of attacks. Furthermore, traditional cryptographic algorithms failed in insuring security once their keys compromised. In order to insure a secure vehicular platform, we introduce in this paper a new decoy technology DT and user behavior profiling (UBP) as an alternative solution to overcome data security, privacy and trust in vehicular cloud servers using a fog computing architecture. In the case of a malicious behavior, our mechanism shows a high efficiency by delivering decoy files in such a way making the intruder unable to differentiate between the original and decoy file.**

Keywords—Vehicular Cloud Computing; Vehicular fog computing; Fog computing; VANET; Cloud Computing; User Behavior Profiling; Decoy technology,

I. INTRODUCTION

Nowadays vehicular organizations oriented their intelligent vehicles to use cloud computing [1] inside roads and street sides, in order to protect their data and take benefits from the services that can be provided by this technology (i.e. IaaS, PaaS, SaaS). VCC Services are generally subscription-based services. VCC [2] consists of shared pool of vehicular resources among end users, devices or vehicles. The vehicles nature and the way cloud computing clusters stored information and personnel data can cause new security challenges. Today's encryption security mechanisms that are used to protect our data over the VCC [3] are not fair enough to stop the unauthorized users or vehicles getting access of original user data. As it is known the previous traditional database system that we have uses are deployed in local network access locally only. With the increasing size and number of the connected vehicles day by day, the emerging new computing models that are used in the VCC [4] such as the distributed vehicular computing technologies And The open access to the database from anywhere around the universe, arises a variety of security problems and specially trust issues. By registering into the VCC community, vehicles and users are ready to excess the resources anytime and anywhere they needed around the world for personnel/organizational work. However, above comfortless involve the risk of data compromise and security. In order to overcome this issue of security and privacy in the VCC, we have introduced our new security mechanism based on Fog Computing [5]. Once vehicles registered in the VCC with our system, users automatically start getting benefits from our services without the need of changing or adding something in their vehicular hardware setup [6].

A. Existing Systems

The existing encryption security mechanisms [7] are generally failed to secure the Smart Vehicular Systems (SVS) from intruders and attackers [8][9]. Mainly, at the time of accessing to an available resource, encryption mechanisms are focus only on the key provided by the user without verifying their identity. Consequently, these mechanisms don't show enough efficiency in terms of ensuring security of the SVS. A huge amount of confidential and private data is stored in the VCC clusters, protecting this information from intruders all over the system is still one of the big existing challenges. After the 330 million twitter user data theft [10] over the cloud computing in 2011, many techniques have been implemented in order the reduce the damage cost that an intruder can do. Recently, once secret keys uncovered during computing operations, UBP and Offensive DT appeared such an efficient technique that successfully achieve the mission of reducing the amount of damage can do.

B. Proposed System

In order to overcome security and trust issues in the VCC, we have proposed an innovated security mechanism based on UBP and a new offensive DT over a fog computing system. Using our mechanism, we monitored and detected the abnormal data access pattern requests. Into our system whenever an intruder tries to get access of original user data,

978-1-5386-7850-3/19/$31.00 ©2019 IEEE

the mechanism automatically generates a decoy file with the same name and scrambling content in such a way it looks original as the targeted file and provide it to the intruder.

II. Proposed Algorithm

This Vehicular fog system will be divided into three major components. In order to achieve our security objectives, each component should include a specific algorithm.

- User behavior Algorithm [2]
- Decoy technology [3]
- File Generation

A. User Behaviour Technology

Mainly UBP started with collecting information about users. Getting data directly from the users the were the older systems strategy to understand the user's behavior, the system asking users about the concerned data needed. as the user is never interested in directly giving the input information, UBP method in our vehicular case, focused on profiling user's data implicitly based on some actions performed by the vehicles. From the security sides, it is a continuously monitoring process that determine whether or not an abnormal access to a vehicle's information is occurring. Depicted behavior-based security mostly used by cops in fraud detection (14). Fraud profile most the time includes:

- Large amount of information requested in no time.
- Multiple try to get login into account.
- How often typically a document read/write.
- Trial password and trial key.

In the following, we will define the algorithm notations of the paper.

- Vehicle (Vi) = V1, V2, V3, V4, V5 .....Vn
- Logdetails (Vim) V1m, V2m, V3m, V4m, V5m .... Vn
- AnonymousActivity (Ai) ["no-certification"," expired-registration"," wrong-identity",]
- Original Files (Gij) G11, G12, G32, G41, G51.....Gnm
- DecoyFiles (Dij) D11, D12, D32, D41, D51 .....Dnm

Algorithm 1: Algorithm For detecting Vehicles Behavior

Result: Detect the behavior of the vehicle V_i
BEHAVIOR 1 ILLEGAL;
BEHAVIOR 2 LEGAL;
$V_i \rightarrow$ Current Vehicle

LogDetails (V_{im}) →

Include all activity of Vehicle (V_i)
while TRUE do
  if Anonymous Activity (A_i) then
    ++Logdetails (V_{im})
  else
    continue;
  end
  if Logdetails (V_{im} > T H RESOLD then
    BEHAVIOR (V_i) = 1
  else
  BEHAVIOR (V_i) = 2
  end
end

B. Decoy Technology

This technology mainly based on an on-demand generation of decoy documents, honey pots and other bogus information to be used for detecting unauthorized access to information and to poison the thief's ex-filtrated information [4]. Serving decoys files may confuse attackers to believe that they have ex-filtrated useful information, when they have not [5]. UBP technology may be integrated with Decoy data to secure a user's data in the Vehicular Cloud Computing.

In the case of an abnormal or unauthorized access to a VCC service is noticed, the cloud system returns decoy information and delivered it in such a way that it completely legitimate and normal. The owner of the information, would readily identify when decoy information is being returned by the Cloud, and hence could alter the Cloud's responses through a variety of means, such as challenge questions, to inform the Cloud security system that it has incorrectly detected an unauthorized access. In the case of an unauthorized access, the VCC security system would deliver unbounded amounts of bogus information to the attacker, thus securing the user's true data from can be implemented by given two additional security features:

1. Validating whether data access is authorized when abnormal information access is detected
2. Confusing the attacker with bogus information that is by providing decoy documents.

Algorithm 2: Algorithm Determine Which File Downloaded

Result: Download the File
BEHAVIOR 1 ILLEGAL;
BEHAVIOR 2 LEGAL;
V_i → CurrentVehicle
LogDetails (U_{im}) →
Include all activity of Vehicle (V_i)
procedure DOWNLOADFILE (V_i, file)
if Vehicle (LEGAL) then
Download → Original File (U_i)
else
Download → Decoy File (U_i)
end

Algorithm 2 explains the Decoy file generation algorithm. Decoy file serves when an unauthorize behavior of a user have been detected. Algorithm 1 predicted the unauthorized behavior using log detail table entry. Once the behavior of the user been changed the flag value corresponding to behavior change.

C. File Generation Algorithm

The DT and UBP have become a very interesting research area. Our system is implemented based on designing an algorithm generating files once an abnormal behavior is being identified using UBP technology. The original file and the generated decoy file content should not be easy to identify, it should be completely different. In order to ensure the legitimate download of the file We store the user file inside a secure database, in such a way that whenever an abnormal behavior is being detected, the original file fail to respond the download request. Storing file in VCC environment has become so important in security vision.

Algorithm 3: Algorithm to Store the file

Result: return Sum Value of stored File
LogDetails (V_{im}) → Include all activity of Vehicle (V_i)
procedure STOREFILE (V_i, file)
Queue q=new Queue ();
q. insert (add all the data element of the file one by one);
sum+= (add all element with respective ASCII value);

if (Sum) then
return Sum
else
Return FileNotStored
end

As we know, in the case that the algorithm 1 predicated user behavior as unauthenticated, the algorithm 2 is responsible to send a decoy file, then the Algorithm 3 start working in order to store the file in database. The way that file is been stored, Algorithm 2 can differentiate between the original file and decoy file. The files that are decoy are encrypted using different hash function. Finally, the key that was generated using algorithm 4 can be used for authentication purpose.

Algorithm 4: Algorithm to calculate HMAC Key

Result: Return the HMAC Key
LogDetails (V_{im}) → Include all activity of Vehicle (V_i)
procedure GENERATEHMACKEY(V_i)
Key=GenerateHmacMD5 (using user credentials
Information)
encrypt Key=E (key, sum);
if encrypt Key) then
return encrypt Key
else
Return NotGenerated
End

III. RESULATS AND ANALYSIS

We have analyzed the given security mechanism on 50 vehicles with a varying of unauthorize behavior possible types. Our main objective behind this simulation was to analyze how we can effectively be able to decide whether the current user behavior is unauthorize or original, on the basis of that we will be providing the file. In the present study, we have used a statistical approach, in which the positive value number is the number of times our security mechanism correctly recognized the attacker and non-attacker. Table 1 describes the main parameters used to evaluate the performance of our security mechanism.

TABLE I. MAIN PARAMETERS USED IN OUR SECURITY MECHANISM

$N(x)$	$M(x)$	*Accuracy*
True Cases: the total number of monitored vehicles	False Cases: the total number of unpredicted behaviors	$\frac{N(x)}{N(x)+M(x)}$

In the figure 1 we presented our simulation table, where we have tested the system with the help of 50 vehicles. In this simulation, each vehicle will try to login into the system twenty times. Our simulation results shown the total false positive value obtained, that clearly mention the number of times we were able to detect the behavior of the user correctly.

The Basis of the comparison between the suggested approach and the approach been defined previously is that initially we try to calculate the false positive on the basis that either we use UBP or DT separately. Using these two techniques together result a greater number of false positive, which could define the superiority of our security mechanism, A graphical illustration of this study comparison is presented in figure 2.

Number of Vehicles	*Positive Value*
5	95
10	196
15	264
20	360
25	425
30	558
35	630
40	664
45	855
50	930

Fig. 1. the accuracy of our mechanism comparing with previous systems

IV. Conclusion

Vehicular cloud computing is generally deployed in the open environments using vehicular networks such as VANET, they vulnerable to an increasing number of data attacks. Insuring the private data security of users over this system is becoming a serious challenging problem. In which, Fog Computing is an architecture that uses edge device to predicate and monitor the user's behavior, in order to provide the security of their data locally. The traditional systems were originally developed using encryption algorithm. In contrast, our system is implemented it with the UBP algorithm along with dynamically generated decoy file system concept. In case if intruder download request of a legal file, then using decoy and UBP techniques in Fog computing we could minimize the cost of damage during insider attacks on the VCC system. Our security mechanism could provide unprecedented level of security in the vehicular networks and the VCC.

Acknowledgment

This work was supported by the University of Moulay Ismail Grant Project ITIC-TRANSPORT.

References

[1] S. Raza, S. Wang, M. Ahmed, and M. R. Anwar, "A Survey on Vehicular Edge Computing : Architecture , Applications , Technical Issues , and Future Directions," vol. 2019, 2019.

[2] T. Mekki, I. Jabri, A. Rachedi, and M. ben Jemaa, "Vehicular cloud networks: Challenges, architectures, and future directions," Veh. Commun., vol. 9, pp. 268–280, 2017.

[3] S. Mallissery, M. M. M. Pai, R. M. Pai, and A. Smitha, "Cloud enabled secure communication in Vehicular Ad-hoc Networks," 2014 Int. Conf. Connect. Veh. Expo, ICCVE 2014 - Proc., pp. 596–601, 2015.

[4] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," Veh. Commun., vol. 9, pp. 19–30, 2017.

[5] M. Mukherjee et al., "Security and Privacy in Fog Computing: Challenges," IEEE Access, vol. 5, pp. 19293–19304, 2017.

[6] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, "Vehicular Fog Computing: A Viewpoint of Vehicles as the Infrastructures," IEEE Trans. Veh. Technol., vol. 65, no. 6, pp. 3860–3873, 2016.

[7] N. Hegde and S. S. Manvi, "Thesis Proposal Summary: Key Management Authentication and Non Repudiation for Information Transaction in Vehicular Cloud Environments," Proc. - 2016 IEEE Int. Conf. Cloud Comput. Emerg. Mark. CCEM 2016, pp. 157–160, 2017.

[8] M. Bousselham, A. Abdellaoui, and H. Chaoui, "Security against malicious node in the vehicular cloud computing using a software-defined networking architecture," in 2017 International Conference on Soft Computing and its Engineering Applications (icSoftComp), 2017, pp. 1–5.

[9] A. Alamer, Y. Deng, G. Wei, and X. Lin, "Collaborative Security in Vehicular Cloud Computing: A Game Theoretic View," IEEE Netw., vol. 32, no. 3, pp. 72–77, May 2018.

[10] J. Song, S. Lee, and J. Kim, "Inference Attack on Browsing History of Twitter Users Using Public Click Analytics and Twitter Metadata," IEEE Trans. Dependable Secur. Comput., vol. 13, no. 3, pp. 340–354, May 2016.

[11] J. A. Iglesias, P. Angelov, A. Ledezma, and A. Sanchis, "Creating evolving user behavior profiles automatically," IEEE Trans. Knowl. Data Eng., vol. 24, no. 5, pp. 854–867, 2012.

[12] R. S. Vyas, "Er Er," vol. 2, no. 2, pp. 1–13, 2013.

[13] M. Van Dijk and A. Juels, "On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing," HotSec'10 Proc. 5th USENIX Conf. Hot Top. Secur., pp. 1–8, 2010.

[14] M. Ben Salem and S. Stolfo, "Decoy Document Deployment for Effective Masquerade Attack Detection," pp. 35–54, 2011.

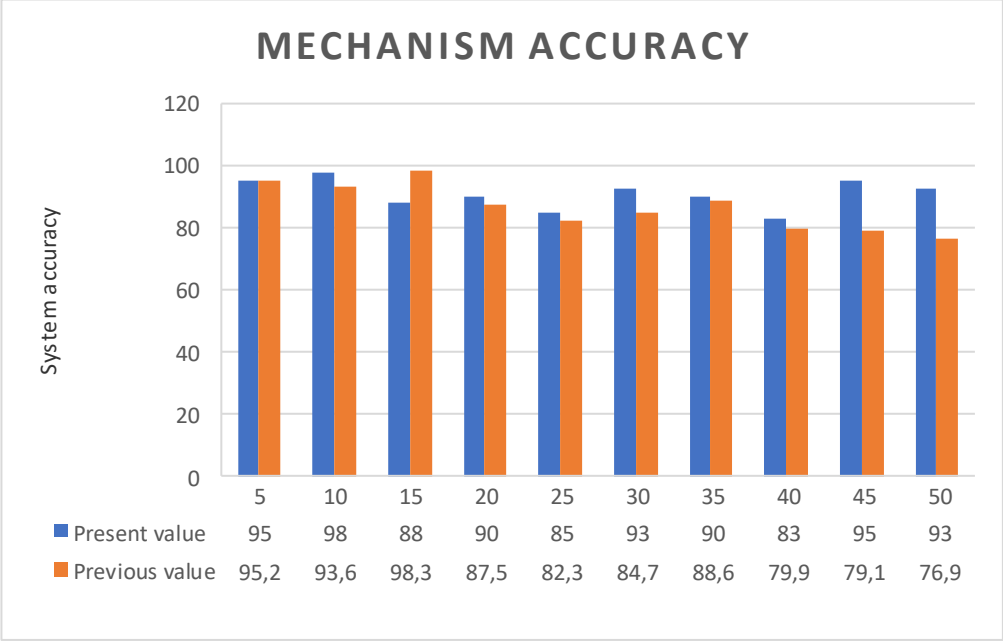

Fig. 2. The proposed algorithm accuracy