Optimizing Cloud Security by Applying New Innovative Filter

MEHDI DARBANDI
Department of Electrical Engineering and Computer Science at Iran University of Science and Technology, IRAN

Abstract: In this paper, at first authors discuss about principles of Cloud Computing and basic concepts of this new and ground-breaking technology. After this brief introduction, they study more about influences of this technology on different industries and products; they specially focus on Amazon products and their future decisions. After that, in the second section, they present new and innovative filter which can be used as an estimator in cloud platforms. Authors claim that if service providers use such innovative algorithms and equip their gateways and routers with such algorithm they are able to estimate and predict about lots of critical criteria's. For example, they can estimate the presence of hackers or race them when they're inside of the network and eliminate them finally or even they can be able to estimate and predict the amount of resources which are need in specific time to prevent from wasting of resources or sudden crashing. Authors of this paper proof their new algorithm by mathematical equations and several simulations at the end of their papers.

Keywords: Cloud platforms security, new innovative Kalman Filter, hacker tracing.

Received: June 25, 2021. Revised: November 29, 2021. Accepted: December 15, 2021. Published: January 3, 2022.

1. Introduction

The importance of virtualized infrastructures and cloud computing is currently increasing rapidly. Virtual infrastructures allow servers, networks, and storage to be virtualized and shared between different users. Cloud computing generalizes and automates this approach such that users of a data center can request virtually any number of machines, networks, and storage while provisioning and scaling is fast and managed transparently by the provider [12].

The increasing complexity and multitenancy of such virtualized infrastructures can cause severe security problems due to possible misconfigurations, e.g. two different users have access to the same storage, and the abstraction of cloud computing hinders the verification of policy compliance. An automated mechanism is required to handle these scenarios and IBM built a prototype for retrieving the configuration of virtual systems and performing certain security analysis on them[12].

Cloud computing has gained remarkable popularity in the recent years by a wide spectrum of consumers, ranging from small start-ups to governments [12]. However, its benefits in terms of flexibility, scalability, and low upfront investments, are shadowed by security challenges which inhibit its adoption. In particular, these highly flexible but complex cloud computing environments are prone to misconfigurations leading to security incidents, e.g., erroneous exposure of services due to faulty network security configurations.

In recent years, Cloud Computing has gained remarkable popularity due to the economical and technical benefits provided by this new way of delivering computing resources, and the pervasive availability of high-speed networks. Businesses can offload their IT infrastructure into the cloud and benefit from the rapid provisioning and scalability. This allows an on-demand growth of IT resources in addition to a pay-as-you-go pricing scheme, which does not require a high up-front capital investment. These benefits are in particular attractive to small businesses, like start-ups, who often have traffic spikes or a steep growth rate, and who prefer to avoid intensive up-front capital investment in their IT infrastructure [12]. However, cloud computing is not limited to such small business. The US government, one of the largest consumers of information technology, is initiating a move of parts of its IT infrastructure into the cloud, in order to reduce costs and gain productivity. These general principles of cloud computing can be implemented on different abstraction levels. While Infrastructure as a Service, such as Amazon EC2, provides virtual machines, storage, and networks, higher abstractions include Platform as a Service as well as Software as a Service that provide the actual web-based applications to end-users [12].

Despite its benefits, Cloud Computing also induces unique challenges in terms of security. Multi-tenancy requires proper isolation of users, the abstraction of the cloud hinders compliance verification of the underlying

architecture, and the sheer complexity of such a system implies a high probability of misconfigurations endangering the overall security. While the benefits of cloud computing are clear and end-users demand such services, security is a major inhibitor of cloud computing adoption on all levels of abstraction. In numerous studies the security related problems have been pointed out. One of the top risks exposed in the study is the failure of isolation in the cloud computing environment [12].

Cloud computing environments are becoming increasingly complex, more tenants are sharing the same physical resources, and the flexibility and possibility of programmatic configurations can lead to unforeseen misconfigurations. For example, network-based storage volumes can be flexibly attached to virtual machines, and potentially a volume will be attached to a wrong virtual machine risking the exposure of sensitive data on t hat volume. Network security is also flexibly managed through a programmatic interface, which could lead to problems resulting in network services exposed wrongly to the public and opening not properly secured services to other peers [12]. Administrators of such virtual infrastructures must be able to easily understand the complex deployments and ensure that proper security is given. The dynamic and agility of such environments also provides a challenge in ensuring the security over its entire lifetime due to their constant changes [12].

In order to successfully address the problem of configuration complexity and potential misconfigurations in cloud computing environments, we narrowed down the problem domain to a specific case of multi-tier applications deployed in infrastructure clouds using a specific cloud provider as an example case. We will study existing literature in the broad domain of virtual machine security, which plays a f undamental part in the security of infrastructure clouds, and network security analysis with a focus on vulnerability assessment and reach-ability [12]. B ased on the insights and inspirations obtained by performing the literature review, we will propose a novel approach in assessing the security of a multi-tier application deployed on the Amazon infrastructure cloud. By implementing our approach and then evaluating it regarding practicality and scalability, we will determine the practical usefulness for detecting misconfigurations even in large-scale deployments. The evaluation is performed both theoretical and practical. The theoretical evaluation is conducted by assuming complex configuration scenarios and analyzes the algorithm run-time using an ideal computer. The practical evaluation is performed using the implementation on a sample multi-tier application deployed on Amazon EC2 [12].

The main contribution of this paper is a novel approach in the security evaluation of multi-tier virtual infrastructures, inspired by vulnerability assessment approaches for traditional computing environments and applied for the case of the Amazon infrastructure cloud. The security evaluation consists of an automated security audit process of the currently deployed configuration with regard to a given policy specifying the desired state of the configuration, and an abstract framework for evaluating the security impact of configuration changes. Besides the main contribution stated above, multiple minor contributions can be pointed out [12]. A comprehensive description of the underlying architecture of the Amazon infrastructure cloud is presented, which was publicly only available in incomplete and fragmented form. We provide a comparison of two methods for deploying multi-tier virtual infrastructures on Amazon with regard to the provided isolation levels [12]. Finally, a data model for representing the configuration of Amazon deployments is presented and integrated into a larger data model capable of representing configurations of different virtualization systems [12].

Cloud computing is a broad term combining several different types of service offerings. In general we distinguish between *Software*, *Platform*, and *Infrastructure* as a se rvice, which are offered by the cloud provider [12]. The main focus of this paper lies on *Infrastructure as a Service*, also called *Infrastructure Clouds*, but for comparison reasons the other types of offerings are also briefly presented [12].

Storage can be provided in different ways varying among the multiple IaaS providers. Four different forms can be identified in the currently available providers: NAS-like, SAN-like, API-based data objects, and Virtual Machine storage. A virtual machine has typically a f ixed-size data storage available, which is equivalent to a hard disk in a regular desktop or server computer. In some cases this type of storage is only intended to be used for temporary data and is itself non-persistent, i.e., after the machine terminates the data is lost [12]. NAS-like storage, like GoGrid Cloud Storage, is accessible from the VMs on a file-based level using standard protocols like CIFS. Amazon Elastic Block Store (EBS) is a SAN-like storage type, which appears to the VM as an additional block-device. An EBS volume can be attached to different VMs, but not to multiple VMs simultaneously, and the size can be adjusted presuming the file system on the block-device is resizable as well.

The last type of storage is accessible through an API and holds data objects up to a specific size, e.g., in the range of several gigabytes. This is a very scalable kind of storage, i.e., one can store an arbitrary amount of objects, and also provides the possibility of distributing these objects using a Content D istribution Network offered by the provider. Examples of this kind of storage are Amazon Simple Storage Service (S3) and RackSpace CloudFiles [12]

2. Performance Comparison of Two Stage Kalman Filtering Technique for Surveillance Permeating Tracking in Cloud Computing [17]:

1. Statement of the Problem:

The problem of interest is described by the discretized equation set [13]:

$$X_{k+1} = A_k X_k + B_k U_k + W_k^x \quad (1)$$

$$U_{k+1} = C_k U_k + W_k^u \quad (2)$$

$$Z_k = H_k X_k + V_k \quad (3)$$

Where $X_k \in R^n$ is the system state, $U_k \in R^m$ and $Z_k \in R^p$ are the input and the measurement vectors, respectively. Matrices A_k, B_k, C_k and H_k are assumed to be known functions of the time interval k and are of appropriate dimensions. Matrix C_k is assumed nonsingular. The process noises W_k^x, W_k^u and the measurement noise V_k are zero-mean white Gaussian sequences with the following covariance's: $E[W_k^x (W_l^x)'] = Q_k^x \delta_{kl}$, $E[W_k^x (W_l^u)'] = Q_k^{xu} \delta_{kl}$, $E[W_k^u (W_l^u)'] = Q_k^u \delta_{kl}$ $E[V_k V_l'] = R_k \delta_{kl}$, $E[W_k^x V_l'] = 0$ and $E[W_k^u V_l'] = 0$, where $'$ denotes transpose and δ_{kl} denotes the Kronecker delta function. The initial states X_0 and U_0 are assumed to be uncorrelated with the sequences W_k^x, W_k^u and V_k. The initial conditions are assumed to be Gaussian random variables with $E[X_0] = \hat{X}_0$, $E[X_0 X_0'] = P_0^x$, $E[U_0] = \hat{U}_0$, $E[U_0 U_0'] = P_0^u$, $E[X_0 U_0'] = P_0^{xu}$.

Treating X_k and U_k as the augmented system state, the AUSKE is described by [13]:

$$X_{k+1|k+1}^{Aug} = X_{k+1|k}^{Aug} + K_{k+1}^{Aug}(Z_{k+1} - H_{k+1}^{Aug} X_{k+1|k}^{Aug}) \quad (4)$$

$$X_{k+1|k}^{Aug} = A_k^{Aug} X_{k|k}^{Aug} \quad (5)$$

$$K_{k+1}^{Aug} = P_{k+1|k}(H_{k+1}^{Aug})'[H_{k+1}^{Aug} P_{k+1|k} (H_{k+1}^{Aug})' + R_k]^{-1} \quad (6)$$

$$P_{k+1|k} = A_k^{Aug} P_{k|k} (A_k^{Aug})' + Q_k \quad (7)$$

$$P_{k+1|k+1} = (I - K_{k+1}^{Aug} H_{k+1}^{Aug}) P_{k+1|k} \quad (8)$$

Where

$$X_k^{Aug} = \begin{bmatrix} X_k \\ U_k \end{bmatrix}, \quad K_k^{Aug} = \begin{bmatrix} K_k^x \\ K_k^u \end{bmatrix}, \quad P_k = \begin{bmatrix} P_k^x & P_k^{xu} \\ (P_k^{xu})' & P_k^u \end{bmatrix},$$

$$A_k^{Aug} = \begin{bmatrix} A_k & B_k \\ 0_{m\times n} & C_k \end{bmatrix}, \quad H_k^{Aug} = \begin{bmatrix} H_k \\ 0_{p\times m} \end{bmatrix}', \quad Q_k = \begin{bmatrix} Q_k^x & Q_k^{xu} \\ (Q_k^{xu})' & Q_k^u \end{bmatrix}$$

Where the superscript 'Aug' denotes the augmented system state, I denotes the identity matrix of any dimension and $0_{m\times n}$ is a $m \times n$ zero matrix. It is clear from (4)-(8) that the computational cost of the AUSKE increases with the augmented state dimension. The OPSKE formulation is based on t he following equations [13]:

$$\hat{\hat{X}}_{k+1|k+1} = \hat{\hat{X}}_{k+1|k} + K_{k+1}(Z_{k+1} - H_{k+1}\hat{\hat{X}}_{k+1|k}) \quad (9)$$

$$\hat{\hat{X}}_{k+1|k} = A_k \hat{\hat{X}}_{k|k} \quad (10)$$

$$K_{k+1} = P_{k+1|k}^x H_{k+1}'[H_{k+1} P_{k+1|k}^x (H_{k+1})' + R_k]^{-1} \quad (11)$$

$$P_{k+1|k}^x = A_k P_{k|k}^x (A_k)' + Q_k^x \quad (12)$$

$$P_{k+1|k+1}^x = (I - K_{k+1} H_{k+1}) P_{k+1|k}^x \quad (13)$$

$$N_{k+1} = [I - K_{k+1} H_{k+1}] M_{k+1} \quad (14)$$

$$\hat{U}_{k+1|k+1} = \hat{U}_{k+1|k} + K_{k+1}^u [\tilde{\tilde{Z}}_{k+1} - H_{k+1} M_{k+1} \hat{U}_{k+1|k}] \quad (15)$$

$$\hat{U}_{k+1/k} = C_k \hat{U}_{k/k} \quad (16)$$

$$K_{k+1}^u = 2P_{k+1|k}^u M_{k+1}' H_{k+1}' \times [3H_{k+1} M_{k+1} P_{k+1|k}^u M_{k+1}' H_{k+1}' + P_{k+1|k}^z]^{-1} \quad (17)$$

$$P_{k+1|k+1}^u = P_{k+1|k}^u + 3K_{k+1}^u H_{k+1} M_{k+1} P_{k+1|k}^u M_{k+1}' H_{k+1}' (K_{k+1}^u)' + K_{k+1}^u P_{k+1|k}^z (K_{k+1}^u)' - 2P_{k+1|k}^u M_{k+1}' H_{k+1}' (K_{k+1}^u)' - 2K_{k+1}^u H_{k+1} M_{k+1} P_{k+1|k}^u \quad (18)$$

$$P_{k+1|k}^u = C_k P_{k|k}^u C_k' + Q_k^u \quad (19)$$

$$P_{k+1|k}^z = H_{k+1} P_{k+1|k}^x H_{k+1}' + R_{k+1} \quad (20)$$

$$P_{k+1|k}^{zu} = H_{k+1} M_{k+1} P_{k+1|k}^u \quad (21)$$

$$\hat{X}_{k+1|k} = \hat{\hat{X}}_{k+1|k} + M_{k+1} U_{k+1} \quad (22)$$

$$\hat{X}_{k+1|k+1} = \hat{\hat{X}}_{k+1|k+1} + N_{k+1} U_{k+1}$$

$$M_{k+1} = [A_k M_k + B_k] C_k^{-1}, \quad k = 2,3,.... \quad (23)$$

$$M_1 = B_0 C_0^{-1}$$

$$N_{k+1} = [I - K_{k+1} H_{k+1}] M_{k+1} \quad (24)$$

2. Performance Evaluations [13]:

To demonstrate the computational advantage of the OPSKE over the AUSKE, the number of arithmetic operations are considered, i.e., multiplications and summations. The arithmetic operations of a standard Kalman estimator with state dimension n and measurement dimension p, are listed in Table 1. It is clear from the equations (4)-(8) and Table 1, that the arithmetic operations required for the AUSKE which has state dimension $n+m$ and measurement dimension

p, are $M(n+m,p)$ for multiplications and $S(n+m,p)$ for summations. Table 2 shows the arithmetic operations of the input estimation and the auxiliary matrices needed by the OPSKE which has state dimension n, measurement dimension p and input vector dimension m. Note that the number of the arithmetic operations of the AUSKE increases with the augmented state dimension, which makes the algorithm computationally inefficient. In contrast, the OPSKE based on the two-stage decoupling technique required fewer computations. The efficiency of the OPSKE is due to order reduction, i.e., implementing two less order n and m partitioned filters. This enables the proposed algorithm to have much better computational efficiency than the AUSKE. So, the arithmetic operations required (AOR) for the AUSKE are [13]:

$$\begin{aligned} &AOR(AUSKE) = M(n+m,p) + S(n+m,p) \\ &= [3(n+m)^3 + 2(n+m)^2 p + 2(n+m)p^2 + p^3 + (n+m)^2 + 2(n+m)p] \\ &+ [3(n+m)^3 + 2(n+m)^2 p + 2(n+m)p^2 + p^3 - (n+m)^2 - (n+m)] \end{aligned} \quad (25)$$

The arithmetic operations required for the input estimation and auxiliary matrices, by the OPSKE as shown in Table 2 and using equations (15)-(24) are

$$\begin{aligned} &AOR(OPSKE) \\ &= M(n,p) + S(n,p) + M^{OP}(n,m,p) + S^{OP}(n,m,p) \\ &= [3n^3 + 2n^2 p + 2np^2 + p^3 + n^2 + 2np] \\ &+ [3n^3 + 2n^2 p + 2np^2 + p^3 - n^2 - n] \\ &+ [3mp + 2m^2 + 2m^2 p + 2mp^2 + p^3 + p^2 \\ &+ 4m^3 + 2n^2 p + 2nm + n^2 m + nm^2 + nmp] \\ &+ [-mp - m^2 - m + 2m^2 p + 2mp^2 + p^3 + 4m^3 \\ &+ 2n^2 p - 2np + p^2 - n + 2n^2 m + nm^2 + nmp] \end{aligned} \quad (26)$$

Using (25) and (26), the operational savings, denoted by OS_{AUSKE}^{OPSKE}, of the OPSKE as compared to the AUSKE are [13]:

$$\begin{aligned} &OS_{AUSKE}^{OPSKE} = AOR(AUSKE) - AOR(OPSKE) = \\ &M(n+m,p) + S(n+m,p) - M(n,p) \\ &- S(n,p) - M^{OP}(n,m,p) - S^{OP}(n,m,p) \\ &= -2m^3 + 15n^2 m + 17nm^2 - 4n^2 p + 6nmp \\ &- 2p^3 + 2np + n - m^2 - 2p^2 - 2nm \end{aligned} \quad (27)$$

And the operational savings of the OTSKE over the AUSKE are:

$$\begin{aligned} &OS_{AUSKE}^{OTSKE} = AOR(AUSKE) - AOR(OTSKE) = -4m^3 + \\ &12n^2 m + 12nm^2 + 4nmp + m - 2m^2 - p^3 - 2nm \end{aligned} \quad (28)$$

Therefore, using (27) and (28) the operational savings of the OPSKE over the OTSKE are [13]:

$$\begin{aligned} &OS_{OTSKE}^{OPSKE} = AOR(OTSKE) - AOR(OPSKE) = 2m^3 + 3n^2 m \\ &+ 5nm^2 - 4n^2 p + 2nmp - p^3 + 2np + n - m + m^2 - 2p^2 \end{aligned} \quad (29)$$

It is clear from (27) and (29) that for m and $p \le n$, the proposed scheme has computational advantage over the AUSKE and it is comparable to the OTSKE. The operational savings discussed here will be tested as an example in the simulation results section. To measure the relative operational savings of the OPSKE with respect to the arithmetic operation required by the AUSKE ($AOR(AUSKE)$), the percentage of the operational savings defined as below:

$$POS_{AUSKE}^{OPSKE} = \frac{OS_{AUSKE}^{OPSKE}}{AOR(AUSKE)} \times 100 \quad (30)$$

Using (27), (29) and (30), the operational savings and the percentage of the operational savings, of the OPSKE comparing to the OTSKE and the AUSKE for different values of n, m and p are shown in Table 3. It can be inferred from Table 3 that the OPSKE has better overall performance than the AUSKE (averaged 32%) and the OTSKE (averaged 7.3%) [13].

Table 1:Standard Kalman Estimator Arithmetic Operation Requirements [13]

	Variable	Number of Multiplications, $M(n,p)$	Number of summations, $S(n,p)$
1	$X_{k+1\|k+1}$	$2np$	$2np$
2	$X_{K+1\|k}$	n^2	$n^2 - n$
3	K_{k+1}^x	$n^2 p + 2np^2 + p^3$	$n^2 p + 2np^2 + p^3 - 2np$
4	$P_{K+1\|k}^x$	$2n^3$	$2n^3 - n^2$
5	$P_{K+1\|k+1}^x$	$n^3 + n^2 p$	$n^3 + n^2 p - n^2$
	Totals	$3n^3 + 2n^2 p + 2np^2 + p^3 + n^2 + 2np$	$3n^3 + 2n^2 p + 2np^2 + p^3 - n^2 - n$

Table 2:Input Estimation and Auxiliary Matrices Arithmetic Operation Requirements for the OPSKE [13]

	Variable	Number of Multiplications $M^{OP}(n,m,p)$	Number of summations $S^{OP}(n,m,p)$
1	$U_{k+1\|k+1}$	$2mp$	$2mp$
2	$U_{K+1\|k}$	m^2	$m^2 - m$

3	K_{k+1}^{u}	$m^2p+2mp^2+p^3+p^2+mp$	$m^2p+2mp^2+p^3-2mp$
4	$P_{K+1\|k}^{u}$	$2m^3$	$2m^3-m^2$
5	$P_{K+1\|k+1}^{u}$	$m^3+m^2p+m^2$	$m^3+m^2p-m^2$
6	$P_{k+1\|k}^{z}$	$2n^2p$	$2n^2p-2np+p^2$
7	$\hat{X}_{k+1\|k}$	mn	mn
8	$\hat{X}_{k+1\|k+1}$	mn	$mn-n$
9	M_{k+1}	$n^2m+m^3+nm^2$	$n^2m+m^3+nm^2-nm$
10	N_{k+1}	n^2m	n^2m-nm
11	$H_{k+1}M_{k+1}$	nmp	$nmp-mp$
	Totals	$3mp+2m^2+2m^2p+2mp^2+p^3+p^2$ $+4m^3+2n^2p+2nm+n^2m+nm^2+nmp$	$-mp-m^2-m+2m^2p+2mp^2+p^3+4m^3$ $+2n^2p-2np+p^2-n+2n^2m+nm^2+nmp$

Table 3:the Operational Savings and the Percentage of the Operational Savings of the OPSKE Compared to the AUSKE and the OTSKE [13]

The state vector dimensions	OS_{AUSKE}^{OPSKE}	POS_{AUSKE}^{OPSKE} (%)	OS_{OTSKE}^{OPSKE}	POS_{OTSKE}^{OPSKE} (%)
$n=4,m=4,p=2$	1340	35.7	592	15.7
$n=4,m=2,p=2$	578	33.7	102	5.9
$n=4,m=2,p=1$	553	37.5	155	10.5
$n=4,m=1,p=1$	242	27.5	23	2.6
$n=4,m=3,p=3$	978	32.7	247	8.2
$n=10,m=2,p=2$	2954	25.1	132	1.12
Average	$\cong 1107$	32.0	$\cong 208$	7.3

3. Simulation Results:

To evaluate the proposed algorithm, an example of maneuvering target tracking problem which turns, in two-dimensional space is simulated such as permeating a hacker into a very important network or databases. In this simulation example, the performance of the OPSKE for the maneuvering target tracking has been compared with the traditional works that done in this concept, as an example of the AUSKE method. As mentioned before in the augmented state method the state vector includes the input vector i.e., acceleration and jerk parameter in maneuvering target tracking problem. The sampling interval is T=0.01 (sec) and target maneuver is applied at 9th second (900th sample). The initial conditions are selected similar for the AUSKE as w ell as the OPSKE. The state vectors are

$X_k=\left[x_k \quad v_k^x \quad y_k \quad v_k^y\right]'$, $U_k=\left[u_k^x \quad j_k^x \quad u_k^y \quad j_k^y\right]'$,

$X_k^{Aug}=\left[x_k \quad v_k^x \quad y_k \quad v_k^y \quad u_k^x \quad j_k^x \quad u_k^y \quad j_k^y\right]'$

Where x_k, v_k^x, u_k^x and j_k^x denote the position, velocity, acceleration and jerk of the target along the x axis, respectively. We consider the target initial conditions for the state and the acceleration vectors as below [13]:

$X_0=\left[2165\,m \quad -80\,m/s \quad 1250\,m \quad 25\,m/s\right]'$,

$U_0=\left[0\,g \quad 0\,g/sec \quad 0\,g \quad 0\,g/sec\right]'$

$X_0^{Aug}=\left[2165\,m \quad -80\,m/s \quad 1250\,m \quad 25\,m/s \quad 0\,g \quad 0\,g/\sec \quad 0\,g \quad 0\,g/\sec\right]'$

The target begins to maneuver as $U_{900}=\left[0g \quad -0.7\,g/\sec \quad 0g \quad 0.4\,g/\sec\right]'$ for $9\ (\sec)\le t\le 90\ (\sec)$.

The system matrices are given by

$$A_k=\begin{bmatrix}1 & T & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & T\\ 0 & 0 & 0 & 1\end{bmatrix},\quad B_k=\begin{bmatrix}T^2/2 & T^3/6 & 0 & 0\\ T & T^2/2 & 0 & 0\\ 0 & 0 & T^2/2 & T^3/6\\ 0 & 0 & T & T^2/2\end{bmatrix},$$

$$C_k=\begin{bmatrix}1 & T & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & T\\ 0 & 0 & 0 & 1\end{bmatrix},\quad H_k=\begin{bmatrix}1 & 0\\ 0 & 0\\ 0 & 1\\ 0 & 0\end{bmatrix}'$$

$$Q_k^u = 2\alpha\sigma_j \begin{bmatrix} T^3/3 & T^2/2 & 0 & 0 \\ T^2/2 & T & 0 & 0 \\ 0 & 0 & T^3/3 & T^2/2 \\ 0 & 0 & T^2/2 & T \end{bmatrix},$$

$$Q_k^x = 2\alpha\sigma_j \begin{bmatrix} T^7/252 & T^6/72 & 0 & 0 \\ T^6/72 & T^5/20 & 0 & 0 \\ 0 & 0 & T^7/252 & T^6/72 \\ 0 & 0 & T^6/72 & T^5/20 \end{bmatrix}$$

$$Q_k^{xu} = 2\alpha\sigma_j \begin{bmatrix} T^5/30 & T^4/24 & 0 & 0 \\ T^4/8 & T^3/6 & 0 & 0 \\ 0 & 0 & T^5/30 & T^4/24 \\ 0 & 0 & T^4/8 & T^3/6 \end{bmatrix}, \quad P_0^x = 10I_{4\times4},$$

$$P_o^u = 0.1I_{4\times4}, \quad P_0^{xu} = I_{4\times4}, \quad H_k^{Aug} = \begin{bmatrix} H_k \\ 0_{2\times4} \end{bmatrix}'$$

$$A_k^{Aug} = \begin{bmatrix} A_k & B_k \\ 0_{4\times4} & C_k \end{bmatrix}, \quad Q_k = \begin{bmatrix} Q_k^x & Q_k^{xu} \\ (Q_k^{xu})' & Q_k^u \end{bmatrix}, \quad P_k = \begin{bmatrix} P_k^x & P_k^{xu} \\ (P_k^{xu})' & P_k^u \end{bmatrix}.$$

Where $\sigma_j = 0.09(ms^{-3})$ the variance of the target is jerk and $\alpha = 0.0123\,(\mathrm{s}^{-1})$ is the reciprocal of the jerk time constant $\tau = 1/\alpha$. T he measurement standard deviations of x and y target positions are: $\sigma_x = 10\sqrt{10}\,(m)$, $\sigma_y = 20\,(m)$. Thus, the measurement covariance matrix is $R_k = \begin{bmatrix} 1000 & 0 \\ 0 & 400 \end{bmatrix}$ for both methods [13]. The Root Mean Square Error (RMSE) index is used for the results evaluation.

Fig. 1 shows the actual value and the estimation of x and y and RMS errors of x and y positions estimations by the proposed OPSKE and the AUSKE. Fig. 2 shows the actual value and the estimations of v^x, v^y and the RMS errors of the x and y velocities estimations by the proposed method compared with the augmented method. The actual value and the accelerations estimations in the x and y directions and their corresponding averaged RMS errors can be seen in Fig. 3.Fig. 4 displays the actual value and the estimated jerk parameters are evaluated by the OPSKE and the AUSKE methodologies [13].

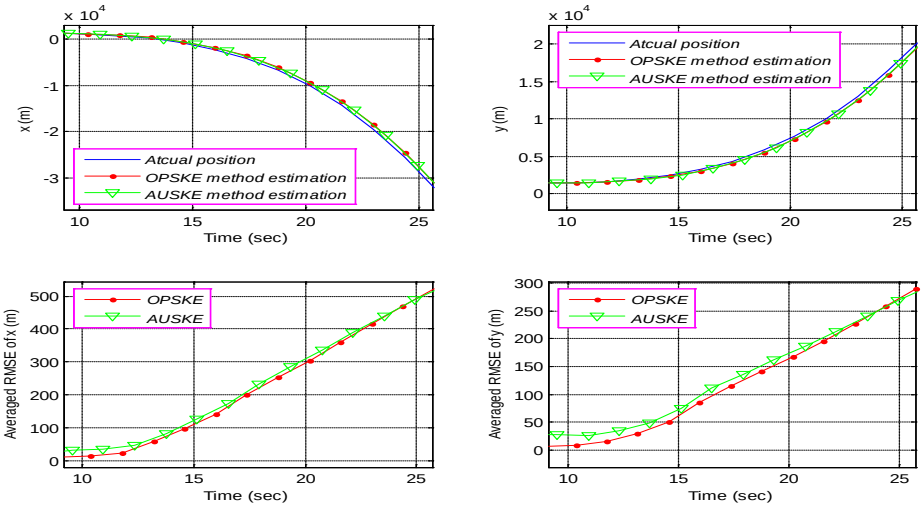

Fig. 1. The actual value and the estimation of the x, y positions and RMS errors estimations by the OPSKE and the AUSKE methods.

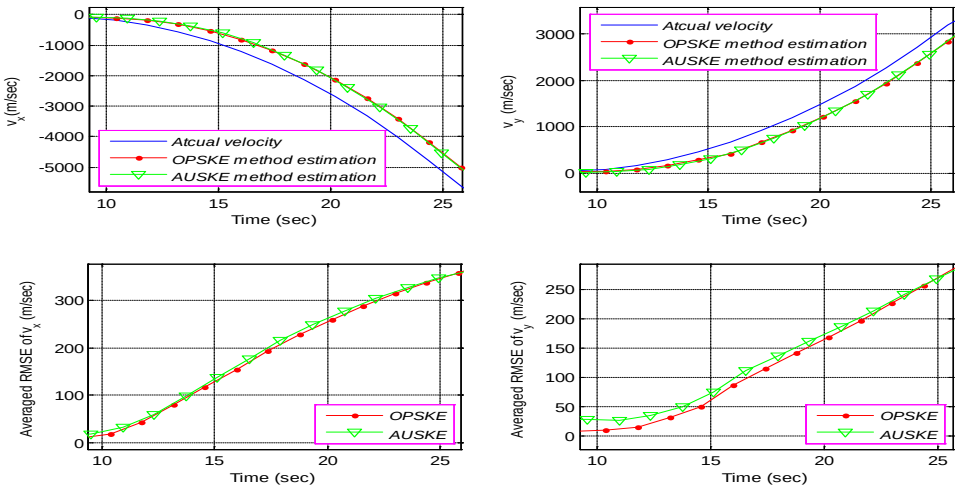

Fig. 2. T he actual value and the estimation of v^x, v^y and RMS errors of x and y velocities estimations by the OPSKE and the AUSKE methods.

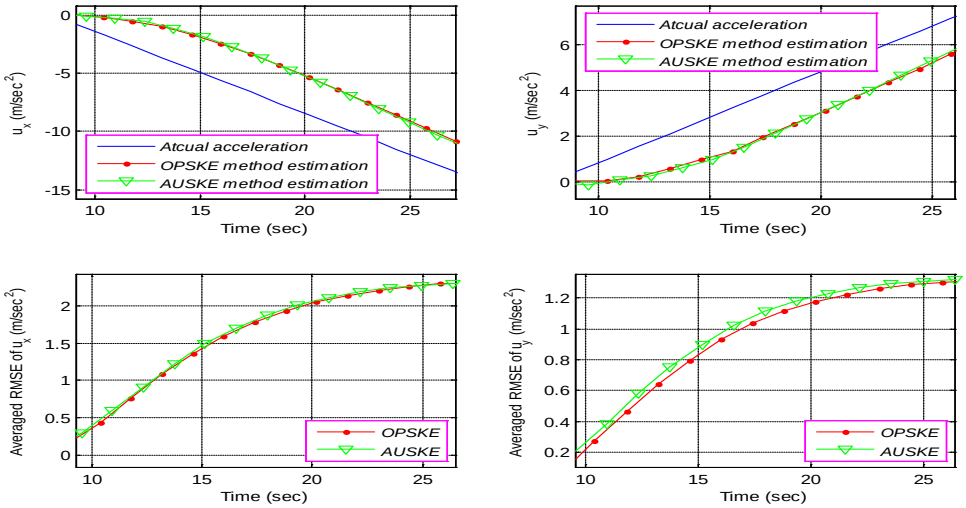

Fig. 3. The actual value and the estimation of acceleration in x and y directions and corresponding RMS errors by the proposed method compared with the augmented methods.

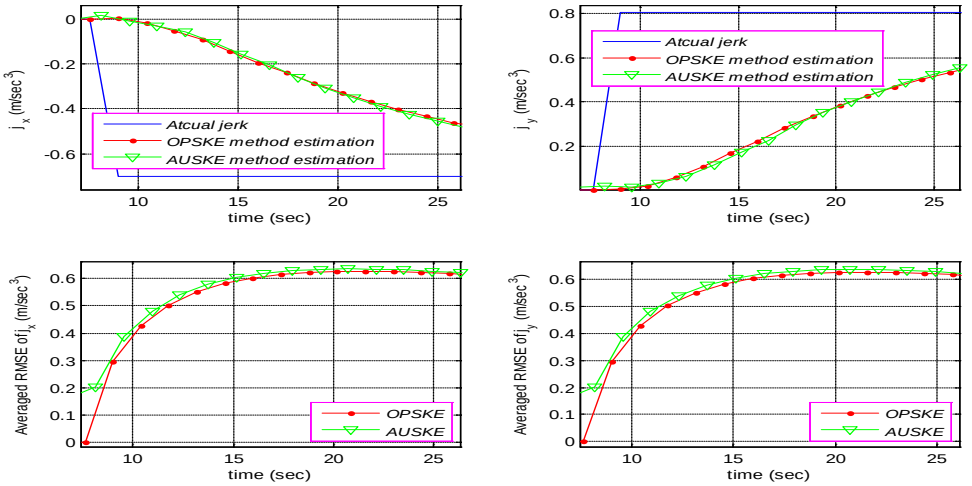

Fig. 4. The actual value and the estimation of jerk parameters and RMS errors by the OPSKE method compared with the AUSKE method.

It is clear that the performance of the proposed OPSKE is as well as the results obtained by the AUSKE in the maneuvering target tracking problem. Note that in this example $n=4$, $m=4$ and $p=2$, and the operation savings for the OPSKE over the AUSKE and the OTSKE as shown in Table 3 a re 1340 (or 35.7%) and 592 (or 15.7%), respectively.

3. Conclusion

In this paper, first of all, authors discuss about different aspects of cloud computing and impacts of this technology on different industries and societies, they study about impacts and influences of this technology with focus to the Amazon products. After understanding this technology and attain more about applications of this technology, they reveal their new and novel algorithm, which is named as two-stage Kalman filtering. Authors claim that by using such algorithm we can estimate and predict about all important factors that are dealing with using of such networks.

References

[1] Mehdi Darbandi "Applying Kalman Filtering in solving SSM estimation problem by the means of EM algorithm with considering a practical example"; published by the Journal of Computing – **Springer**, 2012; USA.

[2] Mehdi Darbandi; "Comparison between miscellaneous platforms that present for cloud computing and accreting the security of these platforms by new filter"; published by the Journal of Computing – **Springer,** 2012; USA.

[3] Mehdi Darbandi; "New and novel technique in designing electromagnetic filter for eliminating EMI radiations and optimization performances"; published by the Journal of Computing - **Springer**, 2012; USA.

[4] Mehdi Darbandi; "Appraising the role of cloud computing in daily life and presenting new solutions for stabilization of this technology"; published by the Journal of Computing - **Springer**, 2012; USA.

[5] Mehdi Darbandi; "Cloud Computing make a revolution in economy and Information Technology"; published by the Journal of Computing - **Springer**, 2012; USA.

[6] Mehdi Darbandi; "Considering the high impact of gettering of silicon on fabrication of wafer designing and optimize the designing with new innovative solutions"; published by the Journal of Computing – **Springer**, 2012; USA.

[7] Mehdi Darbandi; "Developing concept of electromagnetic filter design by considering new parameters and use of mathematical analysis"; published by the Journal of Computing - **Springer**, 2012; USA.

[8] Mehdi Darbandi; "Is the cloud computing real or hype Affirmation momentous traits of this technology by proffering maiden scenarios"; published by the Journal of Computing – **Springer**, 2012; USA.

[9] Mehdi Darbandi; "Measurement and collation overriding traits of computer networks and ascertainment consequential exclusivities of cloud computing by the means of Bucy filtering"; published by the Journal of Computing - **Springer**, 2012; USA.

[10] Mehdi Darbandi; "Unabridged collation about multifarious computing methods and outreaching cloud computing based on innovative procedure"; published by the Journal of Computing - **Springer**, 2012; USA.

[11] Mehdi Darbandi; "Scrutiny about all security standards in cloud computing and present new novel standard for security of such networks"; published by the Journal of Computing - **Springer**, 2012; USA.

[12] MSc. Thesis of Sören Bleikertz*; Norwegian University of Science and Technology; June 2010.*

[13] A. Karsaz, H. Khaloozade, M. Darbandi; "Performance Comparison of the two-stage Kalman filtering Techniques for Target Tracking" Int. IEEE Conf. Harbin, China.