Scientific Research Publishing

Journal of Mathematical Finance, 2019, 9, 402-454
http://www.scirp.org/journal/jmf
ISSN Online: 2162-2442
ISSN Print: 2162-2434

Forecasting the Impact of Information Security Breaches on Stock Market Returns and VaR Backtest

Ilaria Colivicchi[1], Riccardo Vignaroli[2]

[1]Department of Economics and Management, University of Florence, Florence, Italy
[2]European Central Bank, Frankfurt, Germany
Email: ilaria.colivicchi@unifi.it, rvignaroli@gmail.com

How to cite this paper: Colivicchi, I. and Vignaroli, R. (2019) Forecasting the Impact of Information Security Breaches on Stock Market Returns and VaR Backtest. *Journal of Mathematical Finance*, **9**, 402-454.
https://doi.org/10.4236/jmf.2019.93024

Received: June 26, 2019
Accepted: August 18, 2019
Published: August 21, 2019

Abstract

This paper wants to analyse the cyber-risk impact on economy in particular on the returns of the companies suffering information braches. The problem has become very interesting in recent years in the literature for the large dependence of the business with cyber world. The analysis focuses on event study in which the impact of cyber-attacks on stock prices of selected companies is investigated. Cyber-risk phenomenon is processed considering a portfolio of targeted assets, in order to analyse their correlation. Risk measures, such as VaR, will be evaluated and backtested using different methods to monitor which one is able to better capture this type of riskiness.

Keywords

Cyber Risk, Return Correlation, Variance-Covariance Analysis, VaR, Backtest

1. Introduction

The current global context in which companies are involved is very different from the past both for opportunities and threats generated. The proliferation of information technology has affected all economic sectors and, although the internet has often improved the way business is carried out, it has increased the vulnerability of critical infrastructures to information security breaches. When a firm suffers from an information breach, there are immediate direct costs and many residual costs to be incurred. Stock market returns are able to capture implicit and explicit costs of security breaches inside the estimate present value of a firm considering its expected future cash flows. Comparing firm's stock returns after a security breach to the returns prior to the breach, we are able to assess the

effect of it.

The first part of this paper wants to show the impact on share prices of cyber-attack announcements, in particular how informatics braches influence Cumulative Abnormal Return (CAR), and on the level of IT investments to face cyber-security in the period 1995-2018. This part is an empirical update of the previous literature which presents results up to 2015.

In the second part, we want to investigate if it is possible to manage cyber-risk by forecasting the daily portfolio volatility with daily return data according to the fact that the stock market seems to recognize the negative business impacts of a cyber-attack.

Starting from daily return volatility we focus on linear dependence of returns on different portfolio assets. We create a portfolio of assets composed by listed companies in the financial sector, targeted simultaneously by a cyber-attack, to investigate the reaction to these attacks, in terms of different correlation of returns. Correlations are useful to understand moreover which is the impact of cyber-security investment on investor behavior and to investigate if there is a higher or lower correlation among financial entities with different strategies, investments and reactions to past cyber-attacks. The empirical contribution of this paper is to bring out the best model for managing cyber-risk. Different models through which risk managers could evaluate risk measures for different portfolio allocations will be evaluated through an event study. We will diagnose individual models by testing for parameter significance and violations through backtesting procedures as Coverage test (Bernoulli test) and Independence test. Limitations consist in the fact that unfortunately there is no single answer to the problem.

Structure of the Paper

The article is organized as follows. At first, we will present the main literature review dealing with cyber risk and its impact on the returns of a company. After a case study on listed companies will be presented to highlight the impact of the phenomenon on returns considering different time windows compared to the announcement of the security breach. The core of the paper will focus and discuss on different models which risk managers could use to manage the impact of cyber-attack on companies returns. Final remarks will follow.

2. Literature Review

A large number of studies deal with information security breaches, but there is still a limited literature related to the financial sector. Some authors [1]-[14] examine the cyber risk at the national level. [15] and [16], consider the issue of sharing information on computer systems security. [17] and highlight the importance of IT investment. [18] and [19] focus on enterprise cyber risk management, risk mitigation and cyber risk insurance. The economic impact of cyber-attacks is hard to measure. An information security breach can have a negative economic impact, including lower sales revenues, higher expenses, lower

EBITDA, a decrease in future profits and dividends, worsening of reputation and reduction in the market value [20]. It is, therefore, possible that many information security breaches have an insignificant economic impact. [21] outlines that there is a lack of understanding of the different types of cyber-attacks, characteristics and possible results. Some types of cyber-attack are considered as a normal business cost for firms that use information technologies. Moreover, there is a reason to believe that breached firms respond to cyber-attacks by making a new investment in information security [22]. The allocate efficiency of capital markets depends on the extent to which capital asset prices fully reflect information that affects their value [23]. Consequently, the market value represents the confidence that investors have in a firm, and measuring it, we can calculate the impact of a cyber-attack. Moreover, [24] states that investor behavior depends on what they have observed in the past. Several studies [9] [22] [25] use event study methodology to estimate the consequences of cyber-attacks on the market value of breached firms. These studies also consider the type of breach. [22] states that the nature of the breach influences Cumulative Abnormal Return (CAR), while [25] and [9] find that the nature of the attack is not a determinant of CAR. In general, there is a consensus that the announcement of a security breach leads to negative CAR [26]. [27] show that data breaches have a negative and statistically significant impact on a company's market value on the announcement day. [4] finds statistically significant reactions in around 10 days after the news. [28] conducts the analysis over two distinct sub-periods and find that the impact of information security breaches on stock market returns of firms is significant. Some studies [29] [30] [31] present a list of sets of attacks, defenses and effects. [32] states that sometimes cyber-attacks are politically motivated, for example, they are carried out by members of extremist groups who use cyberspace to spread propaganda or attack websites. But information breaches can also be non-politically motivated and in this case, generally, the reason of the attack is financial. Sometimes, cyber-attacks are motivated by socio-cultural issues. Motivations of the attach can be important because can have an impact on the level of attack intensity [33].

[34] highlights the importance of strategies to minimize cyber risk and suggest some techniques to optimize the level of investment in cyber security and insurance for critical infrastructure owners and operators. [35] considers the difficulties to insure cyber risk, especially due to a lack of data and modelling approaches, the risk of change and unpredictable accumulation risks.

[36] highlights the importance of cyber risk for financial and actuarial sector, especially for reputation [37] [38] [39] [40], given that today the banking industry has a significant online presence [41].

Considering CAR is useful even for the fact that we can use some particular properties on financial returns. Extensive research has demonstrated in fact that returns exhibit three statistical properties that are present in most, if not all, financial returns. These are often called the three stylized facts of financial returns

[42]: volatility clusters, fat tails, nonlinear dependence.

The first property, volatility clusters, relates to the observation that the magnitudes of the volatilities of financial returns tend to cluster together, so that we observe many days of high volatility, followed by many days of low volatility.

The second property, fat tails, points to the fact that financial returns occasionally have very large positive or negative returns, which are very unlikely to be observed, if returns were normally distributed.

Finally, nonlinear dependence (NLD) addresses how multivariate returns relate to each other. If returns are linearly dependent, the correlation coefficient describes how they move together. If they are nonlinearly dependent, the correlation between different returns depends on the magnitudes of outcomes.

Modeling correlation dynamics (DCC) is crucial to a risk manager [43] [44]. The idea is that the covariance matrix can be decomposed into conditional standard deviations and correlation matrix, designed to be time-varying.

Orthogonal Garch (OGARCH) transform the observed returns matrix into a set of portfolios with the key property that they are uncorrelated, implying we can forecast their volatilities separately [45].

Literature presented above give an interesting overview on the necessity of the companies to manage cyber-risk and this paper produces some updated results on CAR returns in the last years. In particular, the paper is different from the precedent ones in the second part of the study in which the focus is given to the application of well-known methods to a new type of riskiness and some comments are given about the choice of the best methodology to be used.

3. Analysis on the Dependence of Asset Returns in a Cyber-Breach Window

This research wants to model the nonlinear dependence between returns on different assets during a cyber-attack window.

We refer to cumulative abnormal return (CAR) to accommodate a multiple period event window.

3.1. The Case

We selected a sample from the LexisNexis database, searching for newspaper reports of global cyber-attacks 1995-2018 using different keywords: "information security breach", "cyber-attack", "computer break-in", "computer attack", "computer virus", "computer system security", "bank computer attack", "internet security incident", "denial of service attack", "hacker". We initially identified 321 information security breaches and we registered daily stock market prices adjusted for dividends and splits from the Thomson Reuters DataStream database. Being essential for the study to be available the daily stock prices of the firms, the case finally includes 277 cyber-attacks announcements affecting 149 firms, see **Table 1**.

Following previous studies [22] [27] [29], we run an event study to measure the impact of information security breaches on stock returns. An event study

Table 1. Sample in numbers.

Period of analysis	1995-2018	
Number of cyber-attack registered in the period	321	
Number of listed companies	149	
(Financial companies)	(47)	32% of the sample
Number of cyber-attack to listed companies	277	
(to financial companies)	(96)	35% of the sample

is a method used to measure the effects of an economic event on the value of firms. The null hypothesis is that the event has no impact on the distribution of returns.

The event study methodology makes it possible to verify whether cybercriminals are involved in insider trading. This is important because of the price impact of such a trade [46] and the link between the size of an illegal insider's trade and the value of his private information the probability of detection and the expected penalty if detected [47]. Event study methodology has been widely used in banking and finance literature (see [27] and [48]).

The assumption that the financial markets respond to news affecting the value of a security means that stock market returns are able to capture the implicit and explicit costs of cyber-attacks [28] [49] [50]. In particular, if a firm suffers from an information security breach then it may incur financial losses, which should reflect in its stock price. Stock prices on the days surrounding the event can capture the impact of that event and measure the economic cost of the cyber-attack. Event study methodology is in fact based on a semi-strong version of the efficient market hypothesis [51]. Appraisal of the event's impact requires a measure of the abnormal return (AR) that is the forecast error of a specific normal return-generating mode. Specifically, the AR is the actual ex-post return of the security over the event window minus the normal return of the firm over the event window. The normal return is defined as the expected return without conditioning on the event taking place. In other words, estimated ARs are defined as the company stock return obtained on a given day t, *i.e.* when the cyber-attack is announced, minus the predicted "normal" stock return. We estimate daily AR using the Sharpe (1963) market model, which relates the return of any given security to the return of the market portfolio, assuming that daily common stock returns are described by the market model, which is based on the capital asset pricing model (CAPM). The market model is specified as follows:

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + \varepsilon_{i,t} \tag{1}$$

where:

$R_{i,t}$ = rate of return for firm i on day t;

$R_{m,t}$ = rate of return on the market portfolio on day t;

α_i, β_i = are market model intercept and slope parameters for firm i;

$\varepsilon_{i,t}$ = disturbance term with the usual ordinary least square (OLS) properties,

the random error.

The α_i and β_i coefficients were estimated for each company using an ordinary least square (OLS) regression of $R_{i,t}$ on $R_{m,t}$ for a 121-working-day estimation period (from the 21st to the 141st day before the cyber-attack announcement). This period is the most common choice used in event study (see [52]).

The event window is defined as the time window that takes into account $-\tau_1$ days before and $+\tau_2$ day after the date of the announcement. The date of the announcement is defined as day zero. Following a standard approach, we consider various event windows with different lengths, with the widest lasting from 20 days before the announcement day to 20 days after it. Because our sample includes a large set of firms, we select the following market indexes: The S & P500 Composite, NASDAQ and the S & P600 Small Cap. We use the market index total return as our proxy of $R_{m,t}$. Using the firm-specific parameters estimated for the market model over the estimated period [52], the $AR_{i,t}$, that is the excess return for the common stock of firm i on event day t is measured as follows:

$$AR_{i,t} = R_{i,t} - \left(\alpha_i + \beta_i R_{m,t}\right) \tag{2}$$

The average ($\overline{AR_t}$) for n firm shares on t of the event window is measured as follows:

$$\overline{AR_t} = \frac{1}{n}\sum_{i=1}^{n} AR_{i,t} \tag{3}$$

The concept of Cumulative Abnormal Return is necessary to accommodate a multiple period event window. The CAR from τ_1 to τ_2 is the sum of the included abnormal returns:

$$CAR_i\left(\tau_1,\tau_2\right) = \sum_{t=\tau_1}^{\tau_2} AR_{i,t} \tag{4}$$

where the (τ_1, τ_2) is the event window. The average CAR for the event period $\left[CAR\left(\tau_1,\tau_2\right)\right]$ is measured as follows:

$$CAR\left(\tau_1,\tau_2\right) = \frac{1}{n}\sum_{i=1}^{n} CAR_i\left(\tau_1,\tau_2\right) \tag{5}$$

where n is the number of events.

The statistical significance of CARs using the test statistic Z in [53] to capture the event-induced increase in return volatility as follows:

$$Z = \sqrt{n}\frac{\overline{SCAR\left(\tau_1,\tau_2\right)}}{\sqrt{\frac{1}{n-1}\sum\left(SCAR\left(\tau_1,\tau_2\right) - \overline{SCAR\left(\tau_1,\tau_2\right)}\right)^2}} \approx T\left(0, g/g-2\right) \tag{6}$$

where n is the number of the stocks in the sample and $SCAR\left(\tau_1,\tau_2\right)$ is the standardized abnormal return on stocks i at day t, obtained following [54] approaches as follows:

$$SCAR_{i,t} = \frac{CAR_i\left(\tau_1,\tau_2\right)}{\sigma_i\sqrt{T_s + \frac{T_s^2}{T} + \sum_{i=\tau_1}^{\tau_2}\left(R_{m,t} - T_s\bar{R}_m\right)\Big/\sum_{i=1}^{T}\left(R_{m,t} - \bar{R}_m\right)}} \tag{7}$$

where R_m is the average return on market index in the estimation period, σ_i is the estimated standard deviation of AR on stock i, T is the number of days in the estimation period, T_s is the number of days in the event window and all other terms as previously defined. The Z test in Equation has a t-distribution with T-2 degrees of freedom and converges to a unit normal. Results on our sample are presented in Table 2.

Focusing on the sample of cyber-attacks, we found that the average CARs are negative in all event windows, showing that cyber-attack announcements always lead to negative market returns for a company (the market reacts negatively to the announcement of cyber-attack). The extent of negative market returns, while the statistical significance of mean CARs varies according to the event windows.

In particular, results in the symmetric event windows in relation to the announcement, thus windows: (−20, 20) and (−10, 10), show a high negative mean CAR, even greater than −2.7%. Considering these two-time windows, the statistical significance is very high. It means that we reject the null hypothesis of having a mean CAR equal to zero considering α = 10% for the bigger symmetric window, while we reject the null for the smaller symmetric window considering α = 1%. This result shows that the statistical significance is very high and therefore there is a confidence level at least of 90% in the bigger symmetric window (−20, 20) and it arrives until 99% in the other symmetric window (−10, 10).

The event windows (−5; 5) and (−3; 3) show mean CARs of −0.959% and of −0.758% respectively. This means that significant negative market returns occur on the days prior to and after the announcement of information security breaches. Here again, considering these two-time windows, the statistical significance appears at high level, in fact we reject the null at α = 5%. The confidence level is of 95%, that is a good threshold result and the official announcement of a

Table 2. CAR event study.

Event Window	N. of observations	Mean CAR (%)	Test Z
EW (−20, 20)	277	−2.781	−1.433*
EW (−10, 10)	277	−2.812	−2.637***
EW (−5, 5)	277	−0.959	−2.174**
EW (−3, 3)	277	−0.758	−1.887**
EW (−20, −1)	277	−0.682	−0.429
EW (−10, −1)	277	−0.551	−2.401***
EW (−5, −1)	277	−0.591	−3.779***
EW (−3, −1)	277	−0.478	−3.196***
EW (0, 20)	277	−0.703	−0.436
EW (0, 10)	277	−1.332	−0.528
EW (0, 5)	277	−0.758	−0.366
EW (0, 3)	277	−0.434	−0.340
EW (0, 1)	277	−0.226	0.351

cyber-attack is often partly anticipated by a few days: the asymmetric event windows (−10; −1), (−5; −1) and (−3; −1) show mean CARs of −0.551%, −0.591% and −0.478% respectively. From a statistical point of view there are strong results, we reject the null hypothesis of having a mean CAR equal to zero considering α = 1%. Therefore, the confidence level is of 99%. These results imply that cybercriminals could be implicated in insider trading (as in [27]).

Insider threats (*i.e.* fraud, theft of confidential information and intellectual property, sabotage of computer systems), coming from people within the organization, represent the most prevalent types of cyber threats.

If someone knows in advance certain public information events it can lead to abnormal returns on securities and this situation is typical of insiders who generally have information before the public. A lot of studies have shown that abnormal returns are earned on the basis of the trading behavior of insiders (see [55]).

Furthermore, it must be said that, in the age of globalization, sometimes, it is hard to pinpoint the first release date of an information security breach. It could be interesting to investigate a bit more about insiders on cyber-attack from the moment that significant negative market returns occur on the days prior to the announcement of information security breaches.

Finally, negative market returns also occur on the days after the announcement: the (0; 10) event window shows a mean CAR of −1.332%, but without statistical significance.

In synthesis, the stock market seems to recognize the negative business impacts of a cyber-attack. Effects of cyber-attacks on businesses can be financial, reputational and legal. Some costs are well-known, such as customer breach notifications, post-breach customer protection, regulatory compliance, attorney fees and litigation, cybersecurity improvements, technical investigations. Other costs are less visible, e.g., operational disruptions, loss of intellectual property, lost value of customer relationships, devaluation of trade name increased cost to raise debt, insurance premium increases.

3.2. Some Remarks on Cyber-Attack Effects

We find evidence of an overall negative stock market reaction to public announcements of information security breaches. In the financial sector, we find more negative market returns than other sectors in the event windows before the cyber risk announcements. Thus, could be possible that cybercriminals are involved in insider trading. Moreover, financial entities show greater negative effects on market returns than companies belonging to other economic sectors, hence they should make a bigger investment in IT improving their security. Most mean CARs in the financial sector are statistically significant and higher than in other sectors. This is not surprising given that, beyond protecting data, banks and other financial entities also have the challenge of safeguarding their systems and networks as well as the financial assets they hold, as the recent high biometric security investments implemented by UK banks.

Second, we found that cybercrime may be linked to insider trading. It follows that financial authorities need to strengthen cybersecurity measures. In particular, given the amount of resources currently being devoted by organizations to shore up information security, what is needed is a conceptual framework to help derive an optimal level of information security spending. An economics perspective naturally recognizes that while some investment in information security is good, more security is not always worth the cost. After an attack occurs, an effective cybersecurity incident response is necessary.

The attention is focused even on the social aspect, the reaction to cyber-attacks, in terms of investments by the affected firms, in our case especially banks. There is a reason to believe that breached firms respond to cyber-attacks by making a new investment in information security [22]. The market value represents the confidence that investors have in a firm, and measuring it is a way of calculating the impact of a cyber-attack.

The use of different models to estimate the correlation between the stock prices of companies affected by a cyber-attack will be compared to each other in order to understand, from the point of view of portfolio management and calculation of the VaR, which one performs best and therefore which one may represent the best choice.

3.3. Correlation between Portfolio Asset

We took note of the fact that there has been a cyber-attack of the Distributed Denial of Service (DDOS) type that has taken into consideration 7 English banks, of which 4 listed. We turned the analysis, concerning the correlation between the returns in case of cyber-attacks, in a portfolio management point of view, to verify how and to what extent the returns of these 4 banks are correlated with each other. We implemented a first empirical analysis of the correlations between UK banks like HSBC (HSBA.L), Barclays (BARC.L), Lloyds (LLOY.L) and RBS (RBS.L). We used R-Studio to run the analysis. First of all, we considered a time window from 2012/01/01 to 2018/01/01. Then we obtained the prices and returns of the individual assets. Then we created a matrix corresponding to each vector price of each bank. The object is the returns of each bank, so we made the logarithmic difference of each price vector and we obtain bank stock prices and returns connected to the reference window, as in **Figure 1** and **Figure 2**.

Consequently, we calculated the empirical correlations of the returns of the reference stocks for the time window taken into consideration using the matrix created and then we took the time window of 2017/01/01-2018/01/01 into account and recalculated the correlation between asset returns.

Table 3 and **Table 4**, which represent the various correlations between the returns of the assets of the four banks taken into consideration, are the starting point and comparison basis of the correlation table calculated considering the month of November 2017, the month in which the cyber-attack took place.

Table 3. 2012/01/01-2018/01/01 correlations.

	BARC.L	RBS.L	LLOY.L	HSBA.L
BARC.L	1.000000	0.716533	0.696589	0.595377
RBS.L	0.716533	1.000000	0.689429	0.499121
LLOY.L	0.696589	0.689429	1.000000	0.494083
HSBA.L	0.595377	0.499121	0.494083	1.000000

Table 4. 2017/01/01-2018/01/01 correlations.

	BARC.L	RBS.L	LLOY.L	HSBA.L
BARC.L	1.000000	0.478679	0.465585	0.398640
RBS.L	0.478679	1.000000	0.564220	0.341559
LLOY.L	0.465585	0.564220	1.000000	0.307761
HSBA.L	0.398640	0.341559	0.307761	1.000000

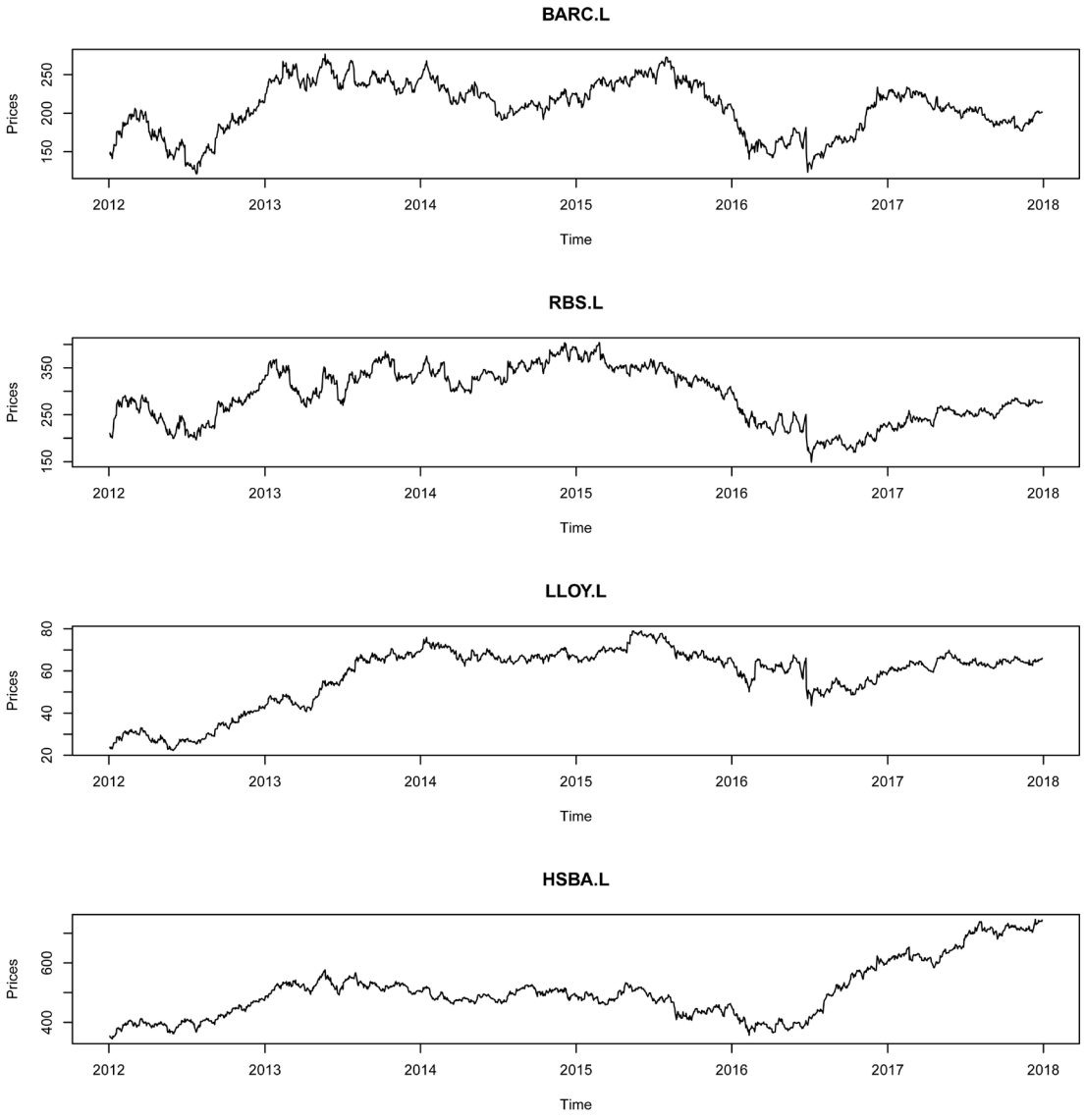


Figure 1. Portfolio asset prices 2012-2018.

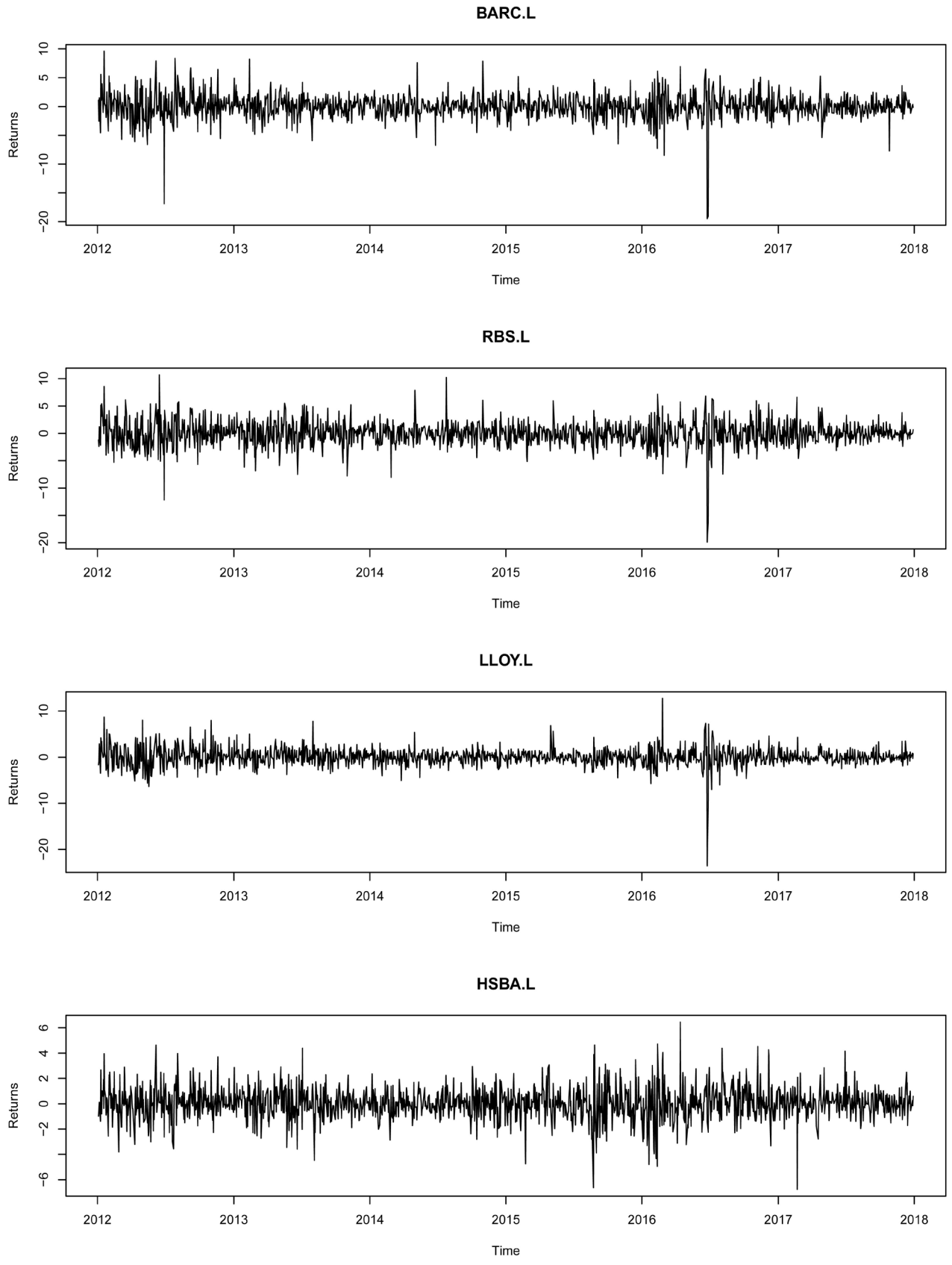


Figure 2. Portfolio asset returns.

Assuming that the market is efficient, the market should react promptly and therefore a negative reaction should be noted as regards both the stock prices of the stocks and thus a greater correlation of the stock returns. This hypothesis stems from the fact that extensive research on the properties of financial returns has demonstrated that returns exhibit three statistical properties. These are often called the three stylized facts of financial returns: volatility clusters; fat tails and nonlinear dependence. Therefore, it is plausible to think that in the time window of November 2017 there is greater volatility and therefore also a greater correlation between the returns of the assets. First of all, we set an annual time window in the code, then we always plotted the graphs of prices and returns for the considered time window.

From Figure 3 and Figure 4 can be seen that there is a very similar trend in November, at least for 3 of the 4 banks considered. Afterwards we will find out why the fourth bank, HSBC UK (HSBA.L), shows a different pattern. Therefore, it is necessary to study the correlations of the returns in order to confirm the hypothesis.

Comparing the correlations between the returns in Table 5 is quite clear the result found: in November 2017, a showcase for the cyber-attack of the DDOS type, three of the four English banks taken into consideration show a greater correlation with respect to the other time windows considered above. Whether a six-year time window (2012-2018) or an annual time window (2017-2018) is considered, the result is always the same. In November 2017 Barclays (BARC.L), Royal Bank of Scotland (RBS.L) and Lloyd (LLOY.L) are much more related.

The result of HSBC (HSBA.L) may come as a surprise because it is countercurrent. The values shown by the correlation of HSBC with other banks in November 2017 are much lower than the other two-time windows considered. The explanation for this lies in the fact that HSBC has been the protagonist of one of the largest operations of technological innovation to ensure greater protection of its customers, their profiles and their passwords. HSBC has taken a big step forward in terms of large-scale cyber security for its customers. The main weapon against cyber-attacks available to banks and their customers seems to be the biometrics of the subject himself. Sharing a series of personal information increasingly precise and unique by the customer seems to be the barrier of the future, the uniqueness of every human being can lead to greater security in terms of identification and then use of the banking service.

Table 5. 2017/11/01-2017/12/01 correlations.

	BARC.L	RBS.L	LLOY.L	HSBA.L
BARC.L	1.000000	0.698607	0.741716	0.004370
RBS.L	0.698607	1.000000	0.779541	0.120150
LLOY.L	0.741716	0.779541	1.000000	0.013745
HSBA.L	0.004370	0.120150	0.013745	1.000000

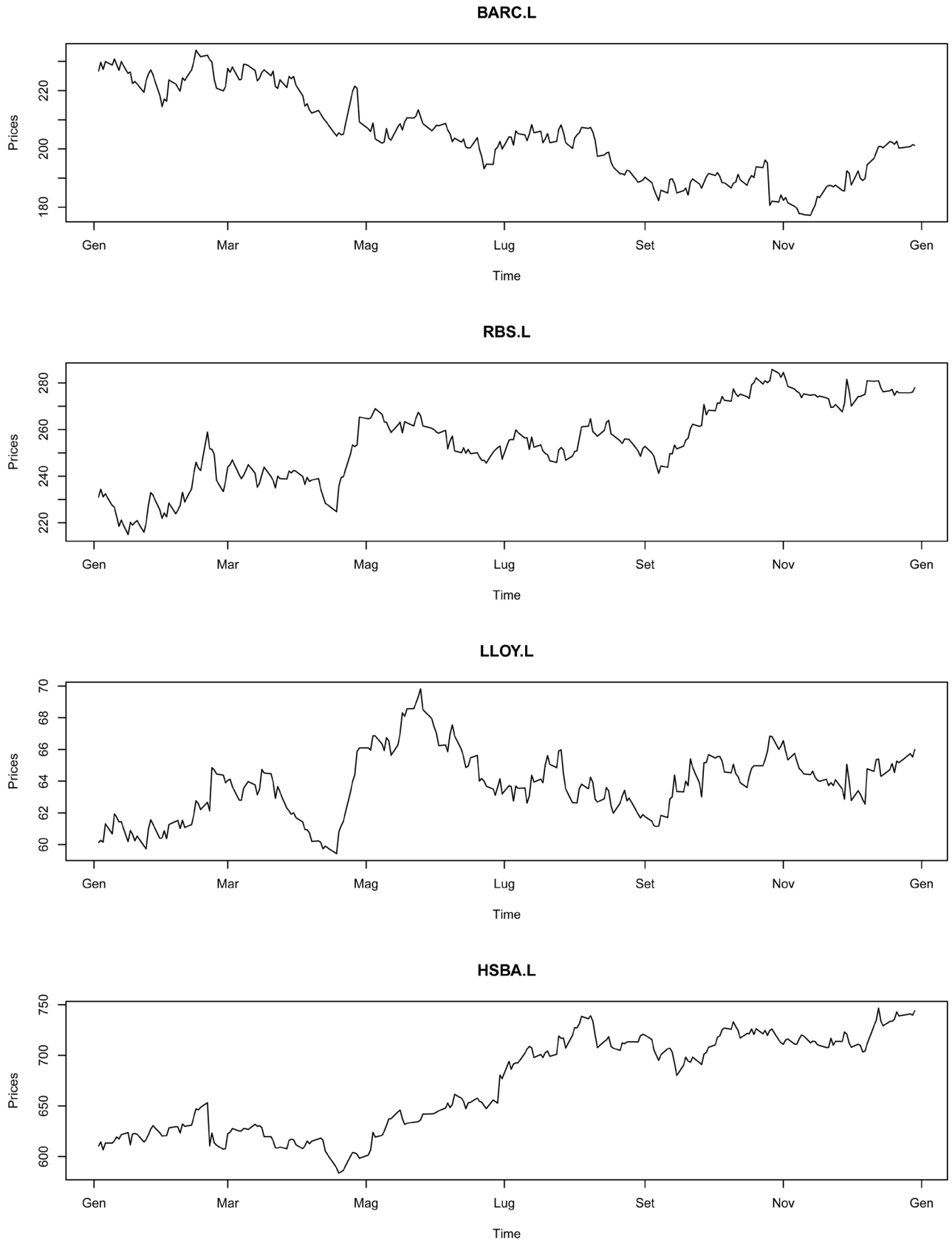


Figure 3. Portfolio asset prices 2017.

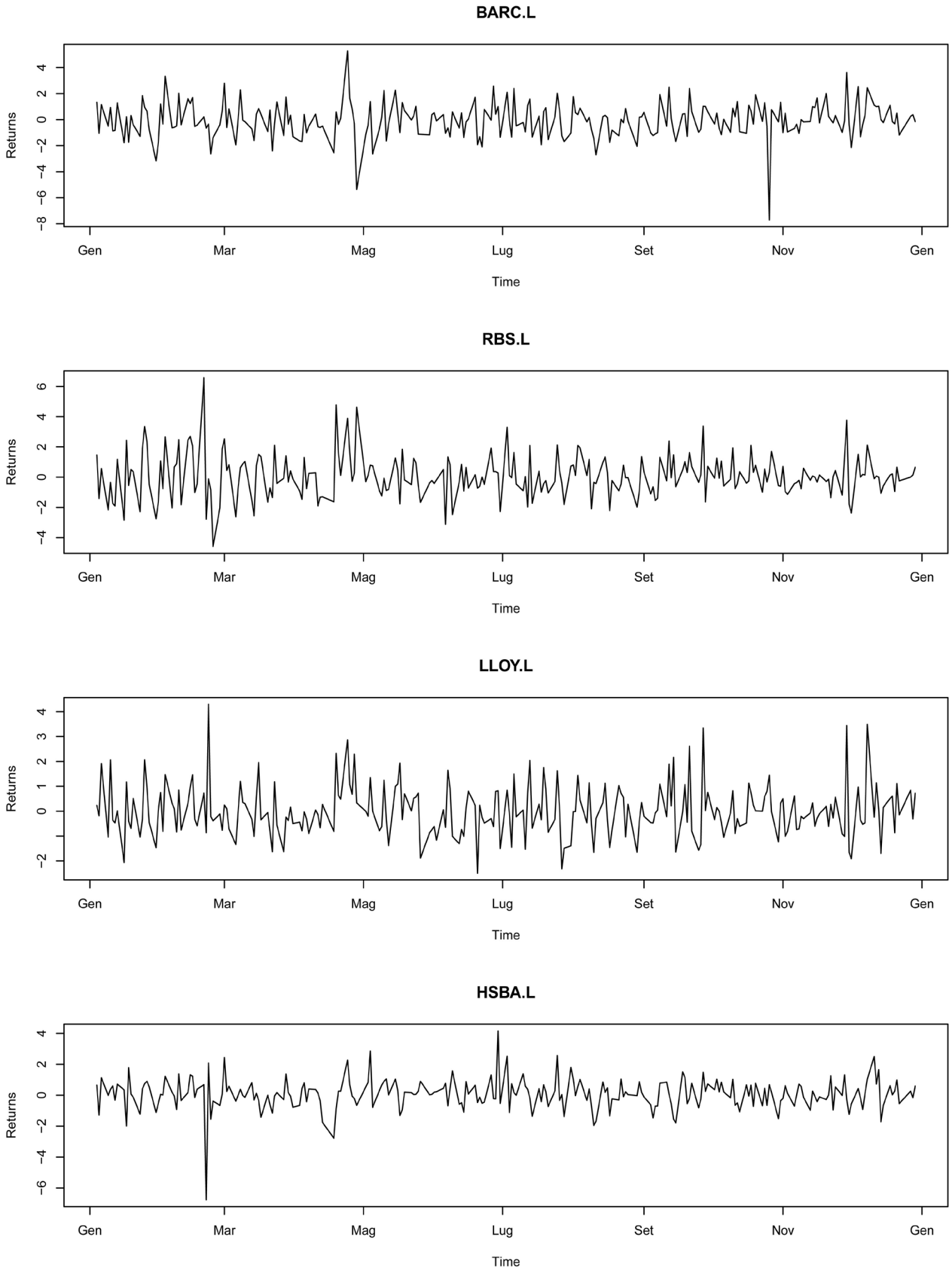


Figure 4. Portfolio asset returns 2017.

HSBC rolled out voice recognition and touch ID services in the summer 2016 in a big step towards biometric banking in the UK. Other banks have also introduced biometric security, but HSBC, which recently suffered an online cyber-attack in January 2016, has been the first to roll it out to millions of retail customers.

3.4. Capacity of Multivariate Models to Estimate the Correlations between the Different Assets

We will consider now the four assets two by two. It is necessary at the beginning to remove their average from the series of returns. At first, we use a simple way to model time-varying covariance relying on plain rolling averages. Using rolling covariance between asset (or risk factor) *i* and *j*, it's necessary to estimate the rolling average covariance choosing m days on which the calculus is based, where m is the number of days used in the moving estimation window. This estimate is very easy to construct but it is not satisfactory due to the dependence on the choice of m and the equal weighting put on past cross products of returns.

Once the covariance has been estimated, the correlations for the reference time window are estimated using the correlation formula. In order to analyze the correlations of the November 2017 time window, we moved the price series and returns in the period 2017/11/04-2017/12/18 so as to have thirty observations of the estimated correlation. If for example m is equal to 4, we obtain the results shown in **Figure 5** and **Figure 6**.

The difference between correlation asset is quite clear, during the estimation window the correlations between the composition of between Barclays, Royal bank of Scotland and Lloyd are higher than the correlations involving HSBC with the other assets as we can see from the graph in the bottom right.

Going ahead we use the EWMA for all the assets, considering them two by two. Firstly, we created a matrix with a number of rows equal to the number of lags (L) considered (*i.e.* 30 L), and two columns for the variances and one for the covariance. We extracted the initial variance-covariance matrix as historical one then we estimated their values using the EWMA model.

From **Figure 7** and **Figure 8** can be seen that in the time window the model also shows that there is a greater correlation between the assets of the reference banks, with the exception of HSBC. We notice that in the first ten days considered there is a downward trend, but if we note the correlation value on the y axis, these values are still much higher than the annual correlations 2017-2018 considered in the previous tables.

Concerning the Orthogonal Garch model we took the sequence of returns and combined by columns creating a matrix. We transformed the return matrix into uncorrelated portfolios. Then we run a univariate GARCH separately to obtain its conditional variance forecast, denoted by Dt. The final step has been the creation of correlation between various assets as reported in **Figure 9** and **Figure 10**.

In this case, we obtain a similar result as using EWMA: a higher correlation for the time window.

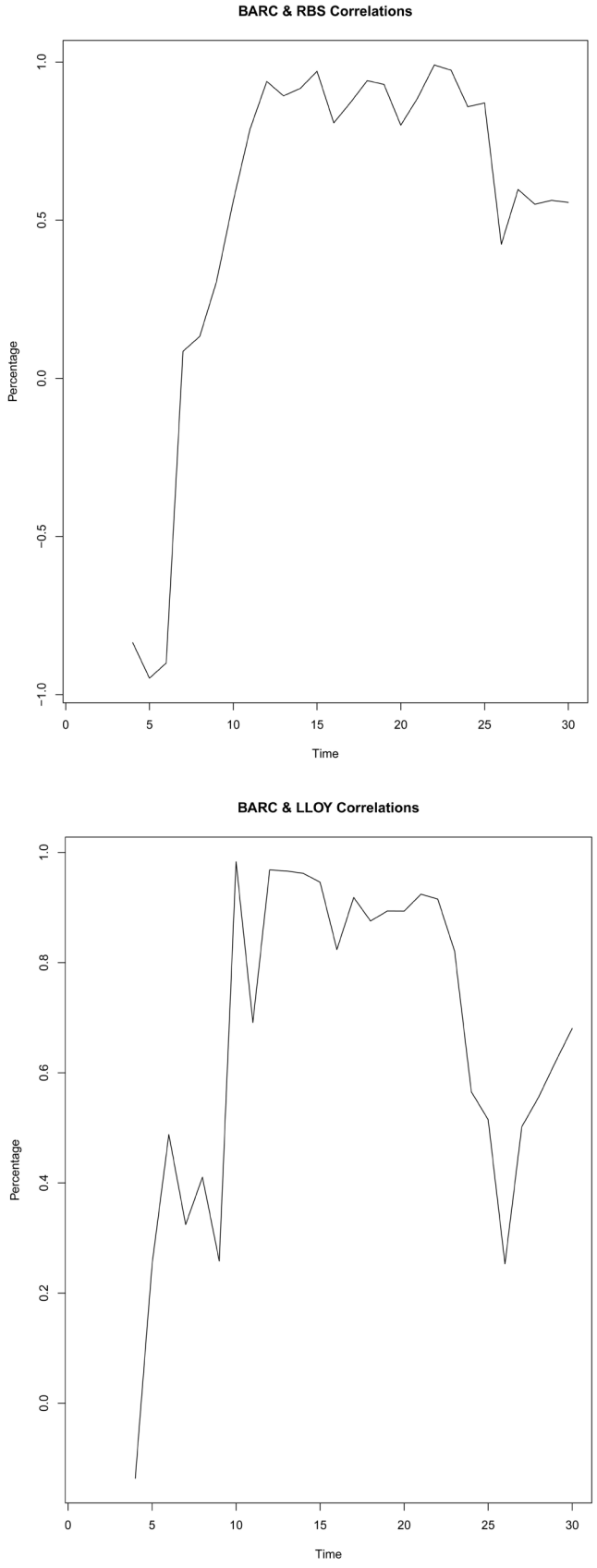


Figure 5. BARC, RBS and LLOY rolling correlations.

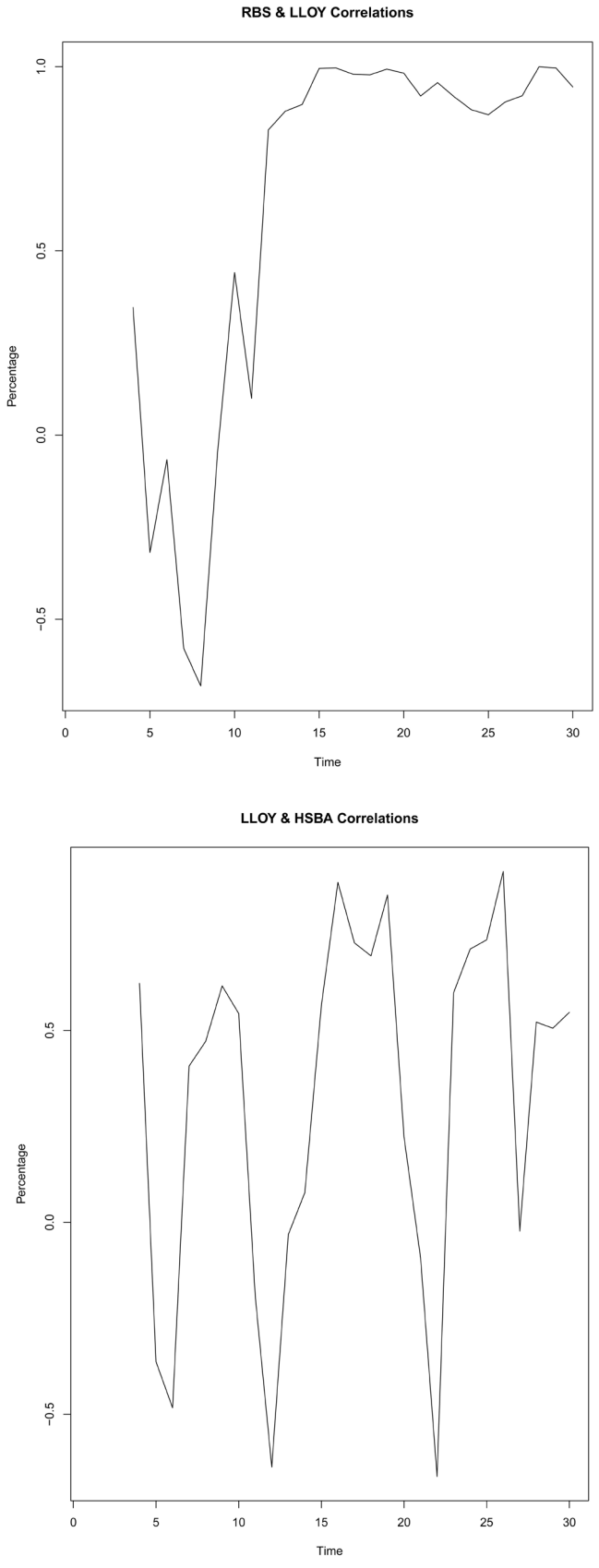


Figure 6. RBS, LLOY and HSBA rolling correlations.

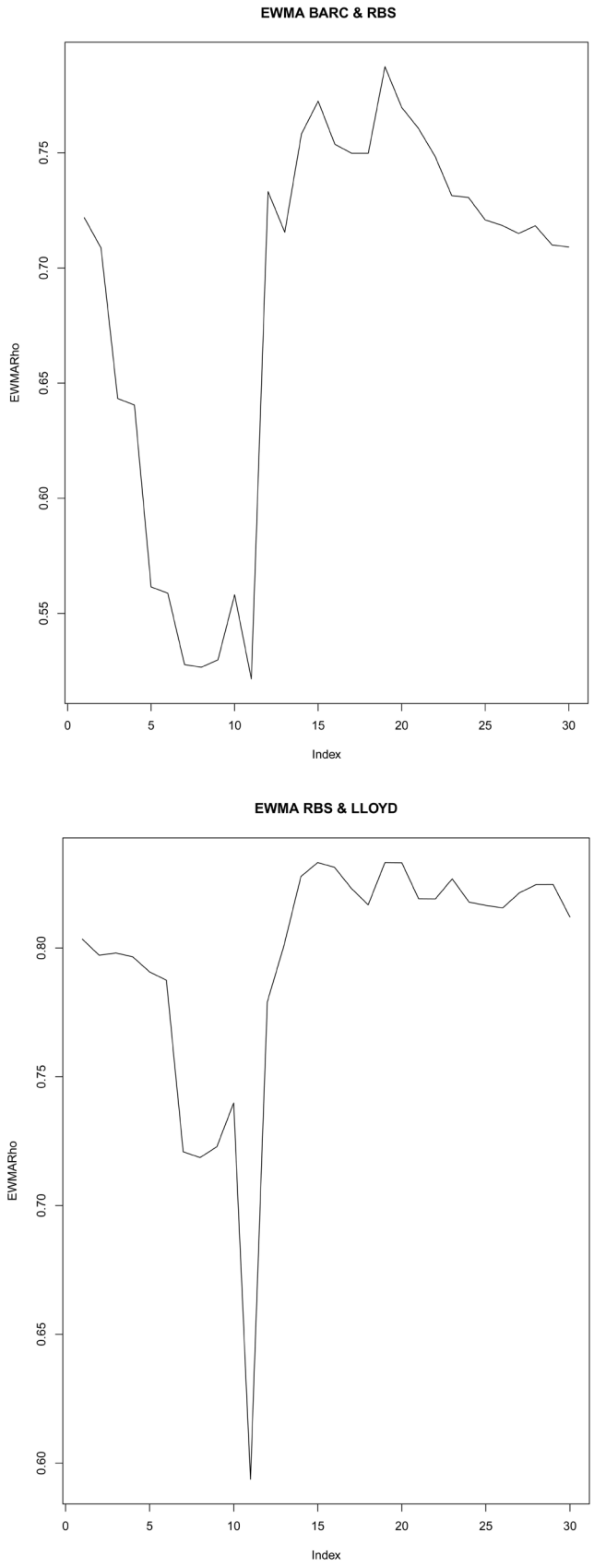


Figure 7. EWMA asset correlations RBS vs BARC and LLOYD.

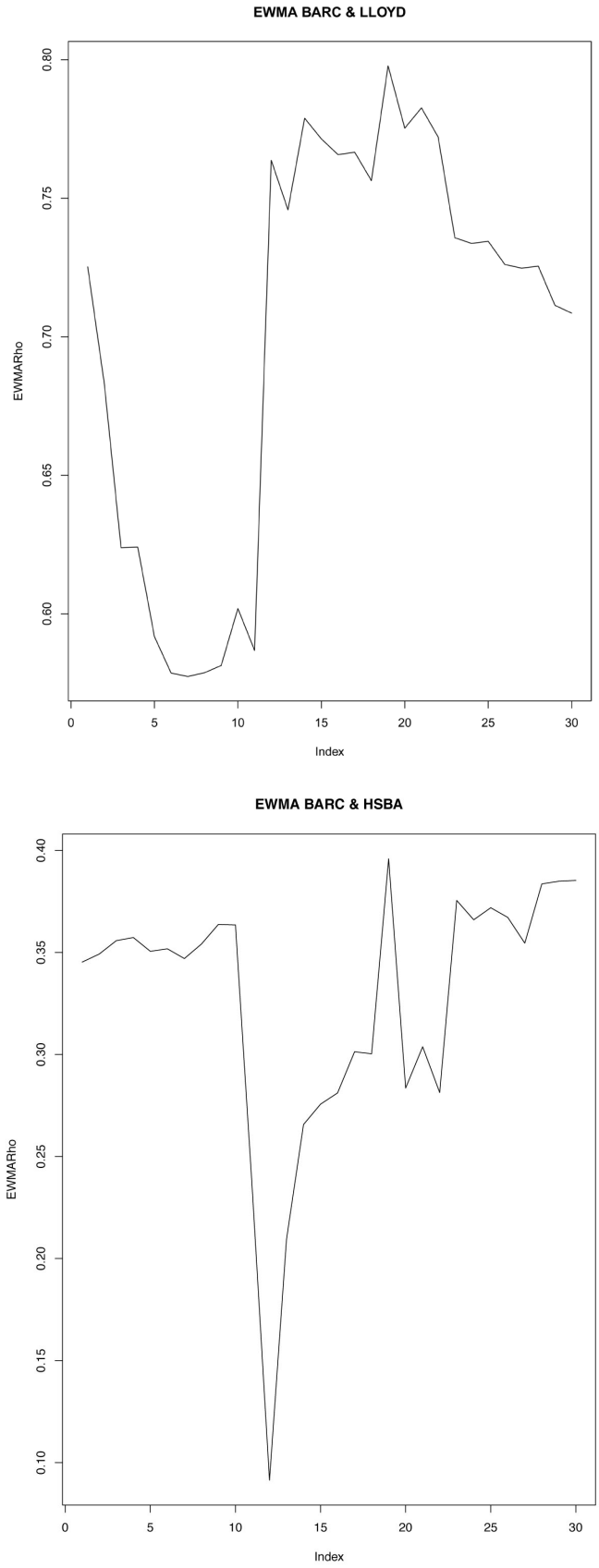


Figure 8. EWMA asset correlations BARC vs LLOYD and HSBA.

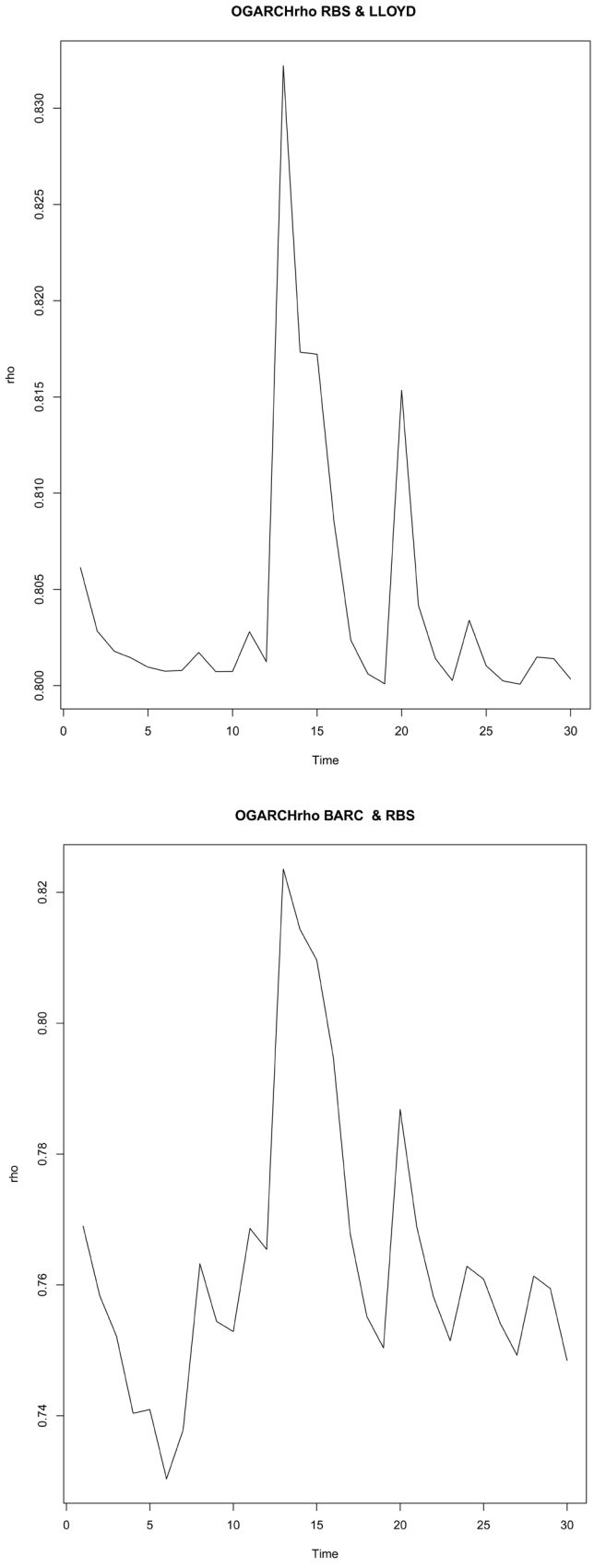
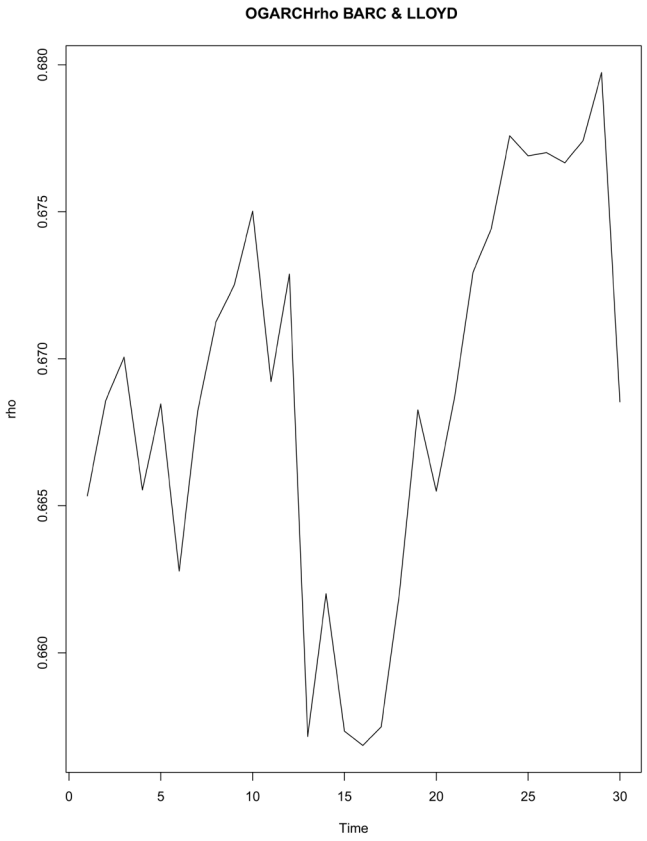


Figure 9. RBS, BARC, LLOY-OGARCH asset correlations.



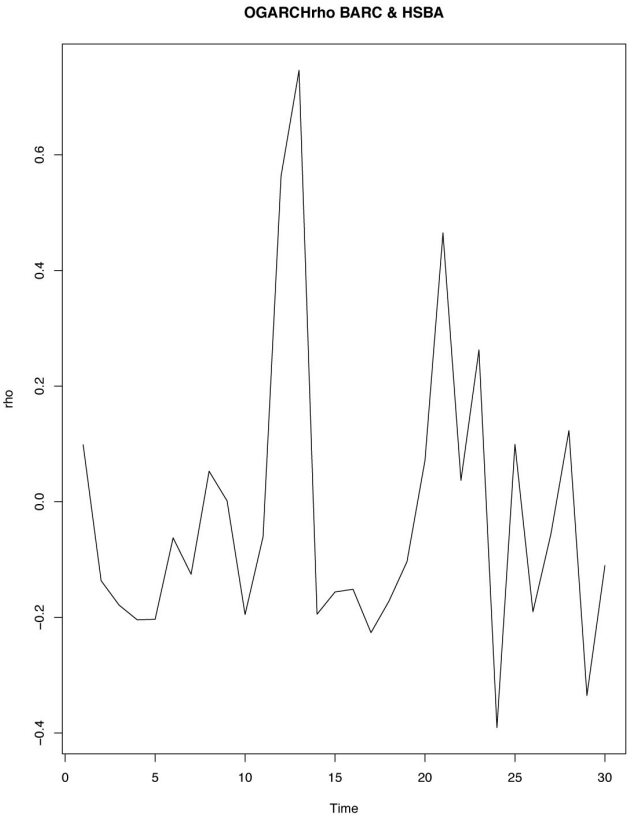


Figure 10. BARC, LLOY, HSBA-OGARCH asset correlations.

The last method considered is DCC. First of all, we estimated univariate GARCH models to get vectors and matrices of starting values. We run the model and we investigated the estimated parameters and the positivity conditions; we extracted the conditional variance estimated by the model, as well as the standardized residuals. We extract the correlation matrix between the two reference assets from the model and plot it in Figure 11 and Figure 12.

Looking at Figure 11 and Figure 12, it is possible to see that even this model, although having a wide volatility, still falls within a very wide percentage range compared to the correlations estimated for the two periods 2012-2018 and for the whole year 2017.

In the following Figures 13-16, we plotted two by two correlations between assets with all four different methods explained above. The window that we have chosen is the time length between 2017/06/01 and 2018/01/01. The attention has to be focused in the last part of the time series on the right where there is the correlation represented by November and December 2017.

There are methods like RollCor and EWMA model that over react to the market impulse while the other methods, like DCC and OGARCH, are smoother. Not surprisingly, both DCC and OGARCH models have more stable correlations, with the OGARCH having the lowest fluctuations. The large swings in EWMA correlations might be an overreaction, but significant compromises are the price paid for tractability by all three models, and all three correlation forecasts reflect these compromises. EWMA model is the easier to implement but is very limited in the type of volatility and correlation dynamics it can capture. The OGARCH and DCC methods are based on separating univariate estimation from correlation estimation. OGARCH is based on estimating a constant correlation while DCC model allows the correlation matrix to be dynamic and therefore is more general. One advantage of the OGARCH approach is that it is well suited to large-scale problems, such as obtaining the covariance matrix for an entire financial institution. What we can say is the fact that DCC and OGARCH, if possibly estimated are the best compromise between facility to be implemented and the response that they give. By the precedent graphs, using any method, is clear that in the last part of the year has been an increasing correlation between RBS, BARC and LLOY. The last figure concerning HSBA shows that the correlation decreased during the last part of the year for the big investment made by the company to protect itself by the security attack that seems to have a positive impact on customers and investors reliance. For this company, the IT investment has been repaid with the market trust. IT investments are able to protect the company by cyber-attack and improve the reputation of the company reducing reputational risk.

3.5. Different Method Comparison

Comparing now the portfolio asset composed by the four banks described above we will stress some results that come from EWMA OGARCH and DCC model. For each graph, we considered only the model correlation between various

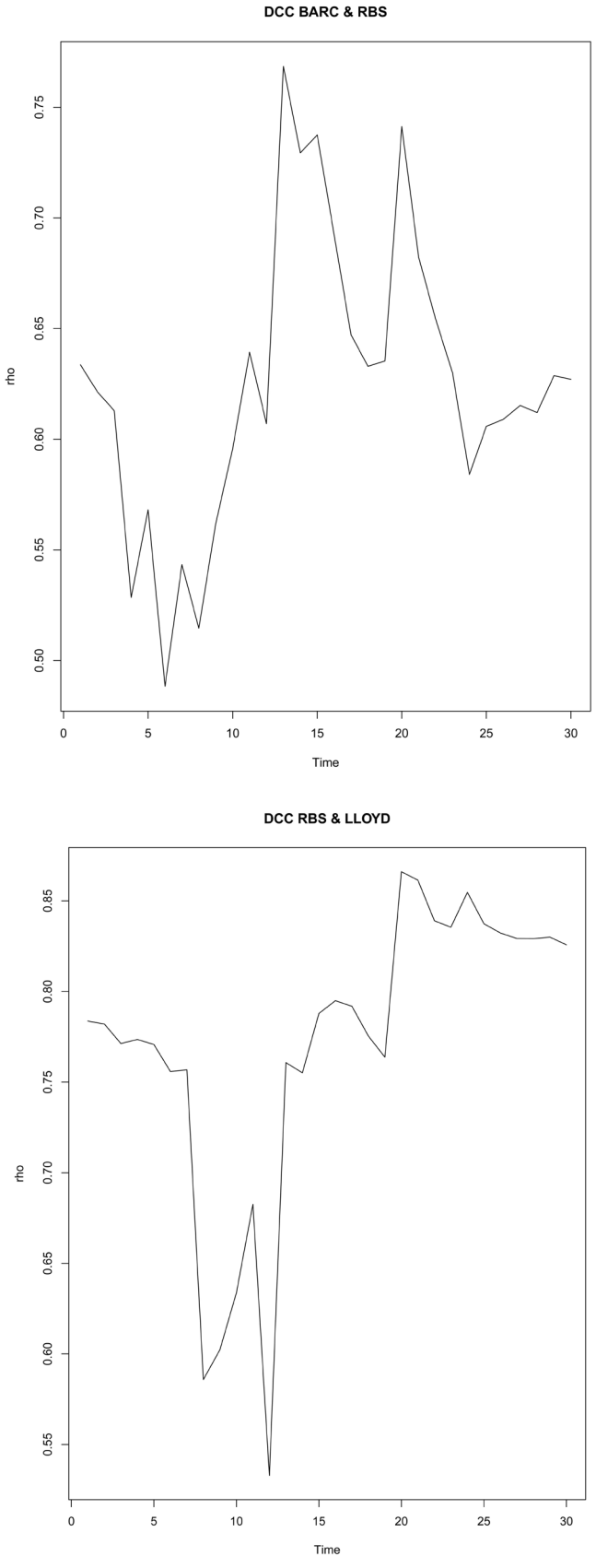


Figure 11. BARC, RBS, LLOY-DCC asset correlations.

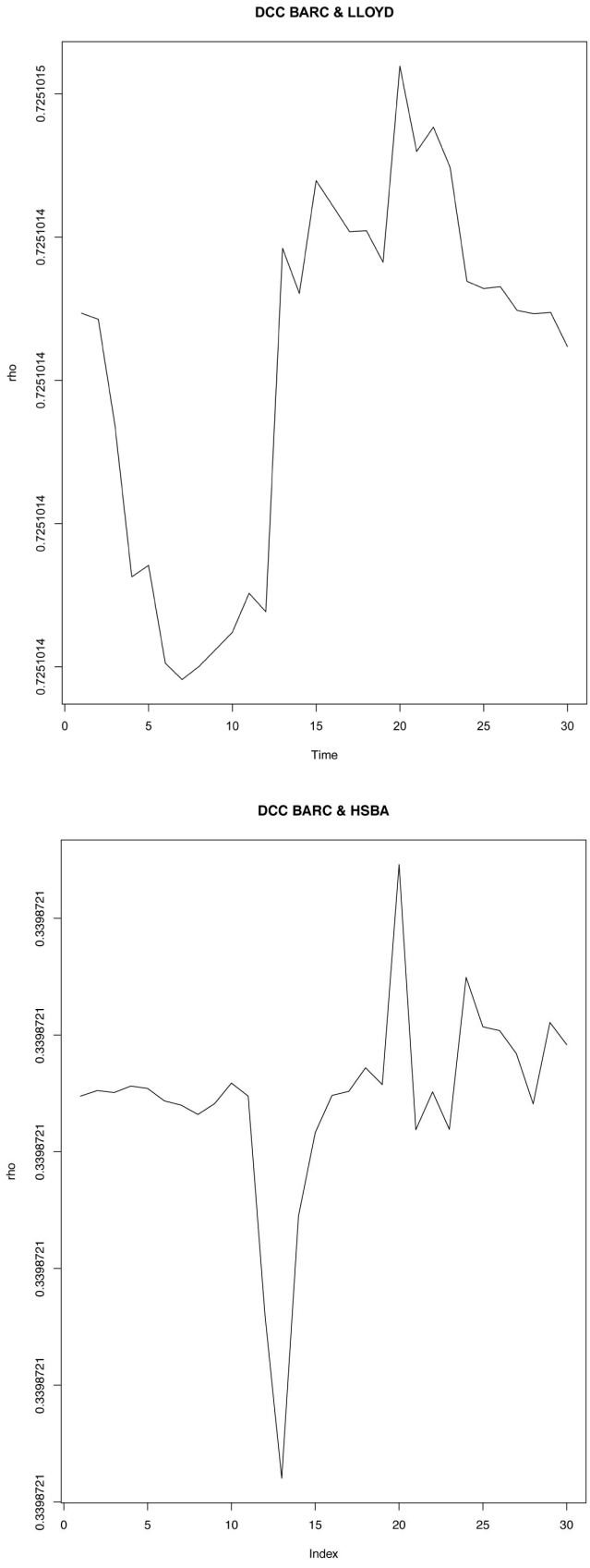


Figure 12. BARC, LLOY, HSBA-DCC asset correlation.

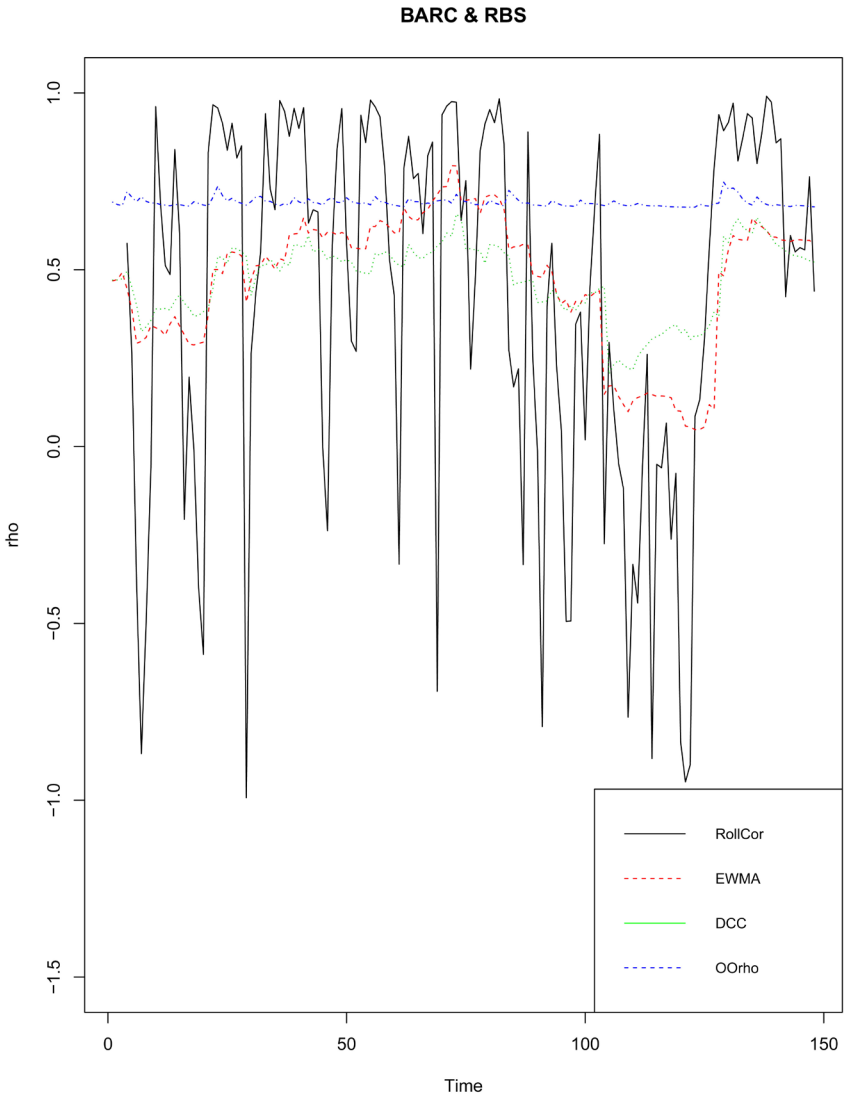


Figure 13. BARC & RBS correlation methods.

couple of assets and not different model in the same graph for the same couple of assets. To do this we created a function to study the correlations between the various assets *i*, *j* for the various time windows. Then we removed the missing values in each price series in order to get a complete list of values, with no missing.

We created a matrix of 4 columns and for each column we entered the historical series of prices taken into consideration. The object of the analysis are the returns and we made the logarithmic difference for each column in order to find them.

We estimated correlations with the same methods: EWMA, OGARCH and DCC.

Starting from EWMA we created a matrix of 16 columns, where each row is a day in the series of returns. This 4×4 matrix correspond to the variance-covariance matrix. So, for every day we made a 4×4 matrix composed by N 4×4 matrices.

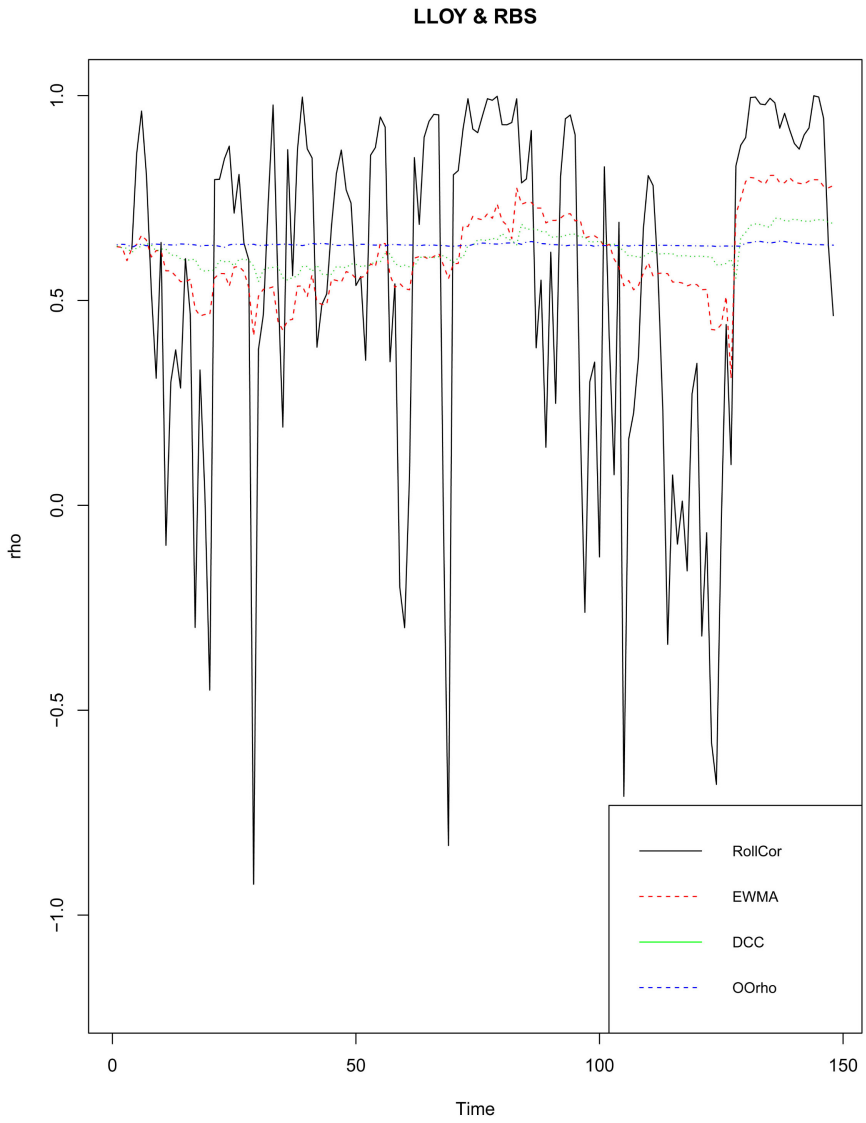


Figure 14. LLOY & RBS correlation methods.

With the same procedure, we created the matrix of squared returns for all considered days of window length. Then we ran EWMA method to find:

$$\widehat{\sigma_{t,ij}} = \lambda \widehat{\sigma_{t-1,ij}} + (1-\lambda) y_{t-1,i} y_{t-1,j} \tag{8}$$

To study the correlations at all times t between each asset, we had to estimate rho by creating N matrices 4 × 4 repositioning the variance-covariance matrix previously estimated within each cell, since:

$$\rho = \frac{COV(i,j)}{\sqrt{VAR(i)VAR(j)}} \tag{9}$$

in order to plot the various correlation graphs.

Figure 17 presents an increasing correlation for all the assets that are not considered with HSBA that is the fourth asset. EWMA correlations concerning HSBA with all the other asset remain quite stable although with some oscillation.

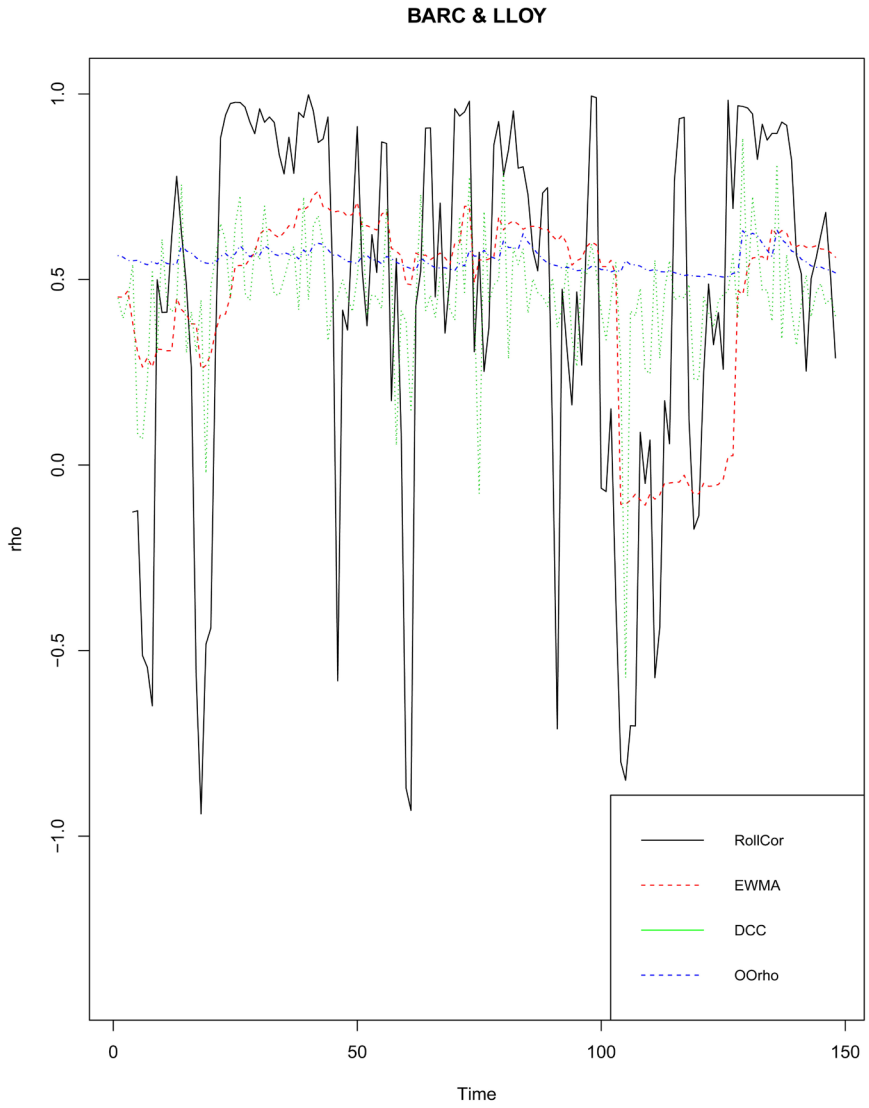


Figure 15. BARC & LLOY correlation methods.

Using OGARCH we estimated the correlations between the various assets and plotted them to notice the differences between the various assets using this method, see **Figure 18**.

We can find a similar case respect to EWMA method. Using OGARCH method concerning November there are bigger oscillation than EWMA model, but Barclays, Royal Bank of Scotland and Lloyd have the bigger correlation between them respect to the combination regarding HSBA.

Following DCC method we estimated univariate GARCH (1, 1) models to get starting values. Then we created vectors and matrices of starting values choosing also parameters weights. We created a matrix with different correlation, each row corresponds to time lag while each column to each asset; so, in this matrix each column represents correlation between two assets. This matrix is the starting point to extrapolate each column of interest and plot them graphically. To keep going this method is necessary to take a bigger time lag, thus we considered

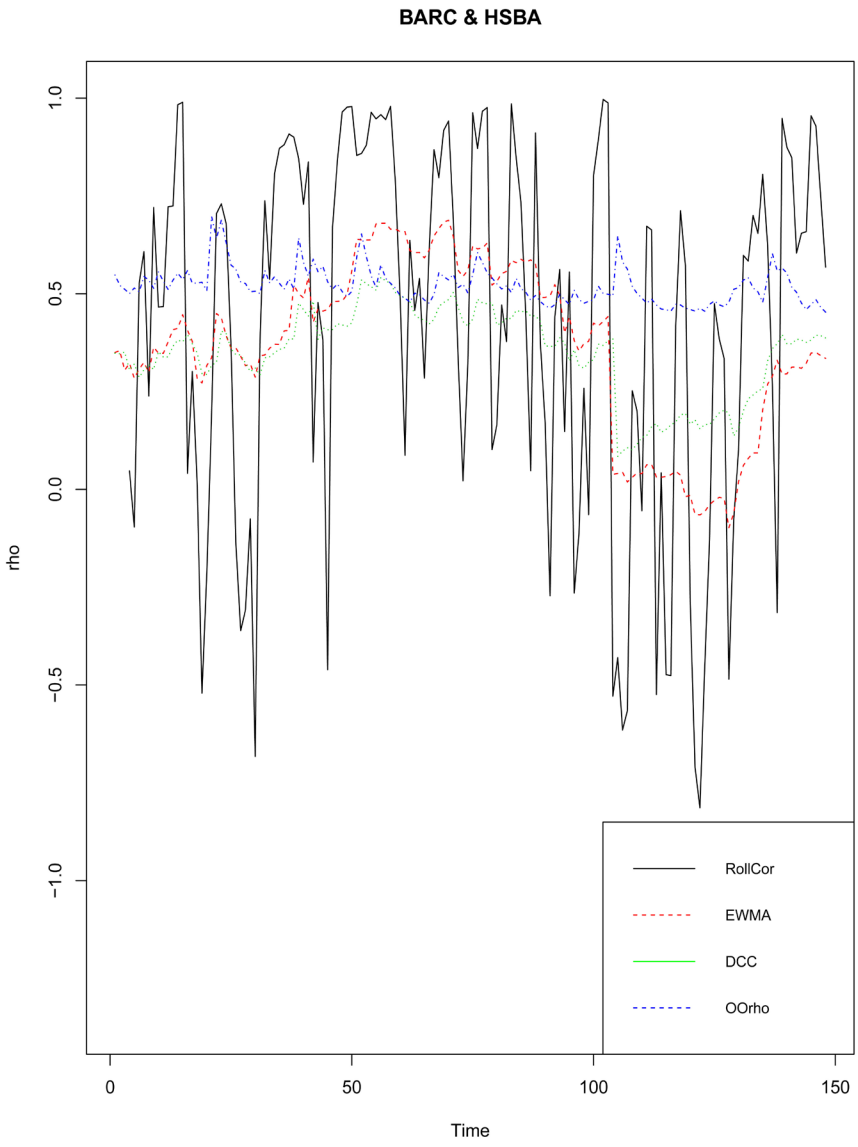


Figure 16. BARC & HSBA correlation methods.

more days using in this case the starting point as 2017/06/01 until 2018/01/01, instead of November 2017 only, see Figure 19. Then we plotted, in Figure 20 and Figure 21, also the other methods correlation (EWMA and OGARCH) to make a comparison of long run.

The typical characteristic concerning DCC and OGARCH method is to be smoother, as is possible to notice looking at the graphs above, while EWMA model overreact at market situations with many oscillations, thus is more peaked.

3.6. Implementing Risk Forecasting

There are two main methods for forecasting VaR: nonparametric and parametric. Non-parametric risk forecasting generally refers to historical simulation (HS), which uses the empirical distribution of data to compute risk forecasts. No

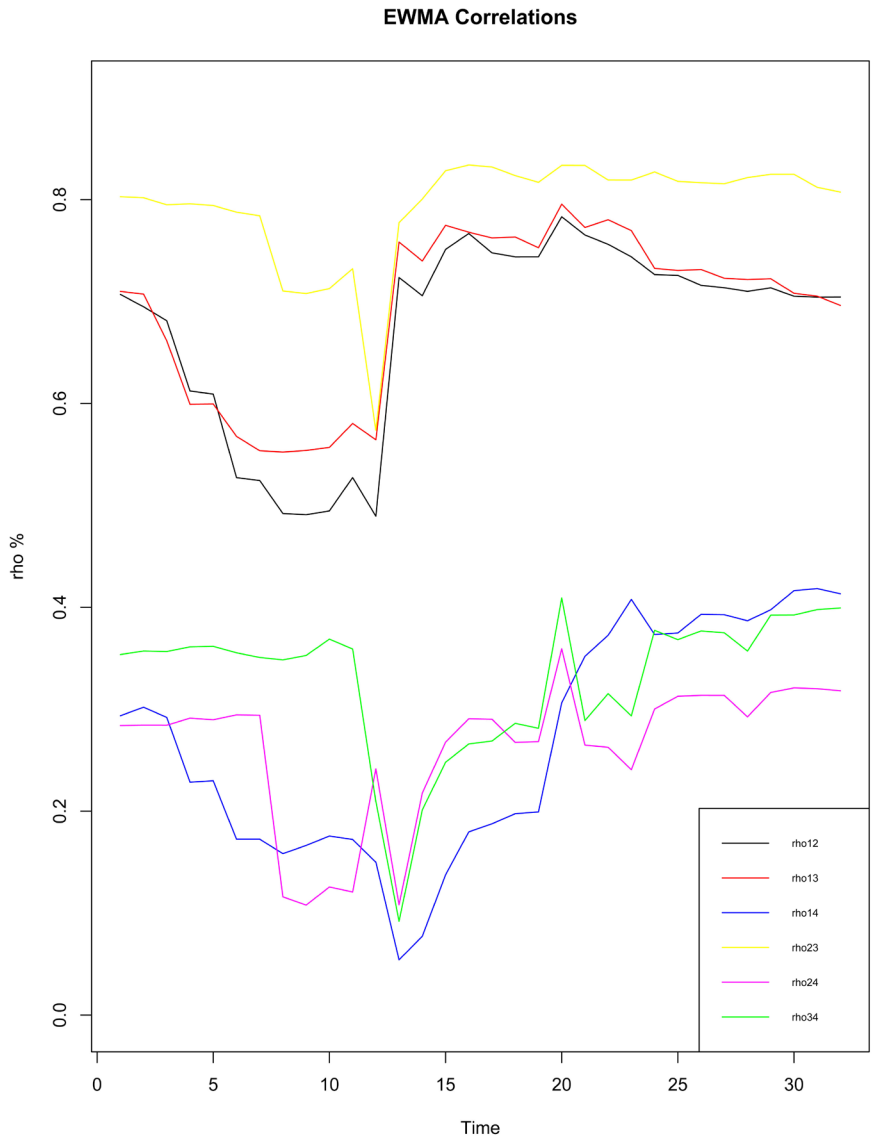


Figure 17. EWMA method portfolio correlations.

statistical models are assumed nor are any parameter estimates required for nonparametric methods. By contrast, parametric methods are based on estimating the underlying distribution of returns and then obtaining risk forecasts from the estimated distribution. For most applications, the first step in the process is forecasting the covariance matrix. The methods used for forecasting the covariance matrix typically include MA, EWMA or GARCH. They are frequently used with the normal distribution and occasionally with the Student-t, but other conditional distributions may also be used. The parametric approach is often referred to as the variance-covariance (VCV) method. Historical simulation (HS) is a simple method for forecasting risk and relies on the assumption that history repeats itself, where one of the observed past returns is expected to be the next period return. Each historical observation carries the same weight in HS forecasting. This can be a disadvantage, particularly when there is a structural break

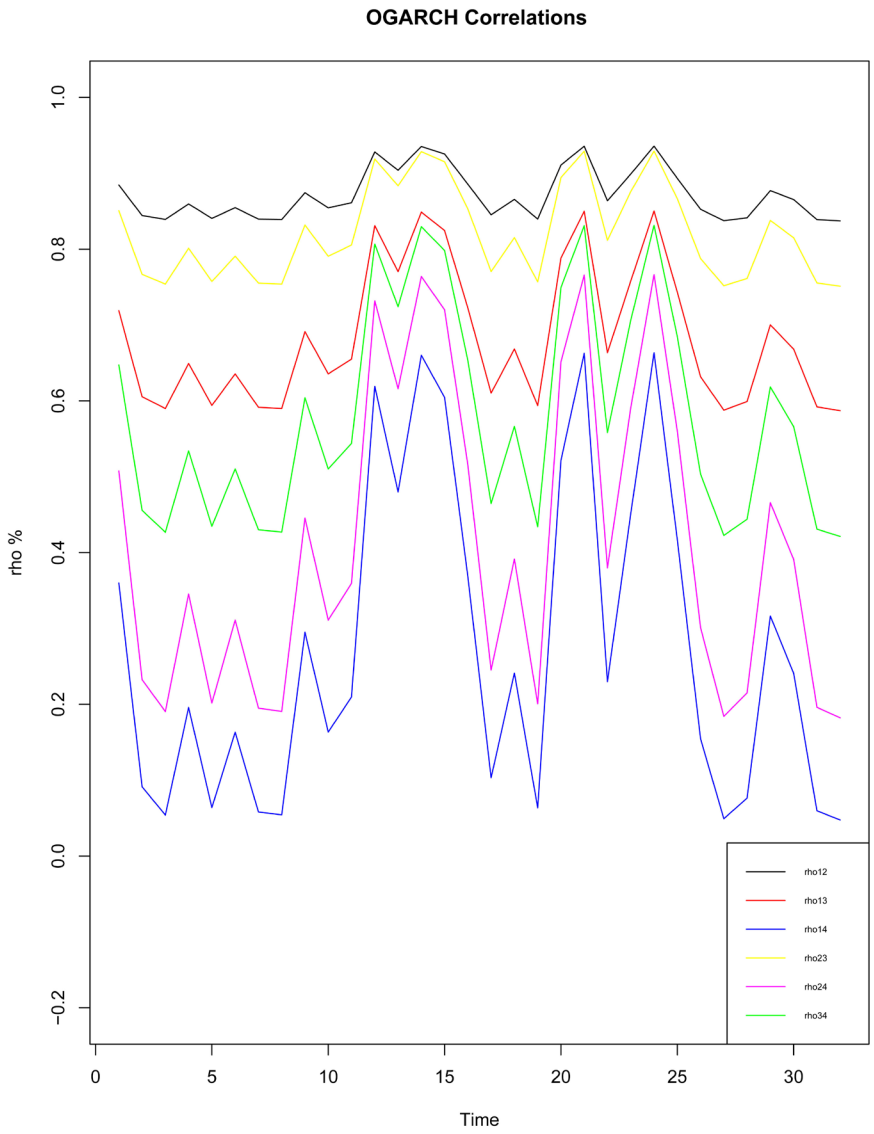


Figure 18. OGARCH method portfolio correlations.

in volatility. However, in the absence of structural breaks, HS tends to perform better than alternative methods. It is less sensitive to the odd outlier and does not incorporate estimation error in the same way as parametric methods. The advantages of HS become especially clear when working with portfolios because it directly captures nonlinear dependence in a way that other methods cannot. We calculated the VaR and the ES for the first day of December 2017 through historical simulations taking as a reference three-time windows, one 2012/01/01-2017/12/01 and two smaller time windows, namely 2017/01/01-2018/01/01 and also 2017/11/01-2017/12/01. The other two important things that we choose have been the portfolio size (1000) and the value to invest in each asset, that we put as 25% for each one. Moreover, it is important to keep in mind what the theory suggests about time windows, that is about their consistency and quality of result. In fact, concerning VaR bigger window sizes have both advantages and disadvantages. The

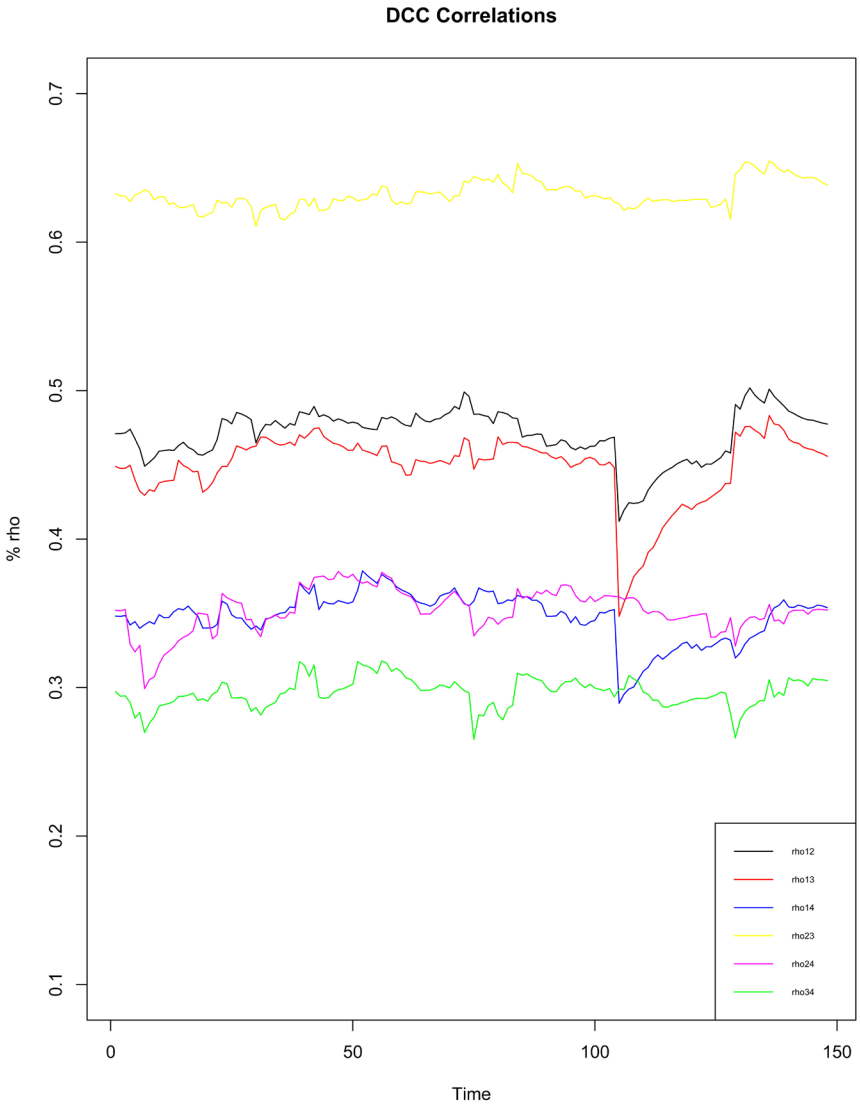


Figure 19. DCC portfolio correlations from 2017/06/01 to 2018/01/01.

advantage is that they are less sensitive to one-off extreme observations, while the disadvantage is that VaR forecasts take longer to adjust to structural changes in risk. Furthermore, very old data are unlikely to be representative of current market conditions. So, in this case as general rule, the minimum recommended sample size for HS is 3/p, where we choose p = 5% and then the minimum window size should be around 60 observations. Concerning ES window length, a minimum of 10 observations are recommended to calculate ES with HS, which means to have 200 sample window observations. Once the time windows and the probability used were set, we created a vector of portfolio weights of the four assets, multiplied the returns by the assigned weights and sorted the returns in ascending order for all the windows, as shown in **Figure 22**.

For each asset, the first window length is about 1496 lags for the portfolio. Then multiplying the portfolio lags by the probability, we obtain 75 values that are bigger than portfolio VaR value. Using the estimation of one year we got 233

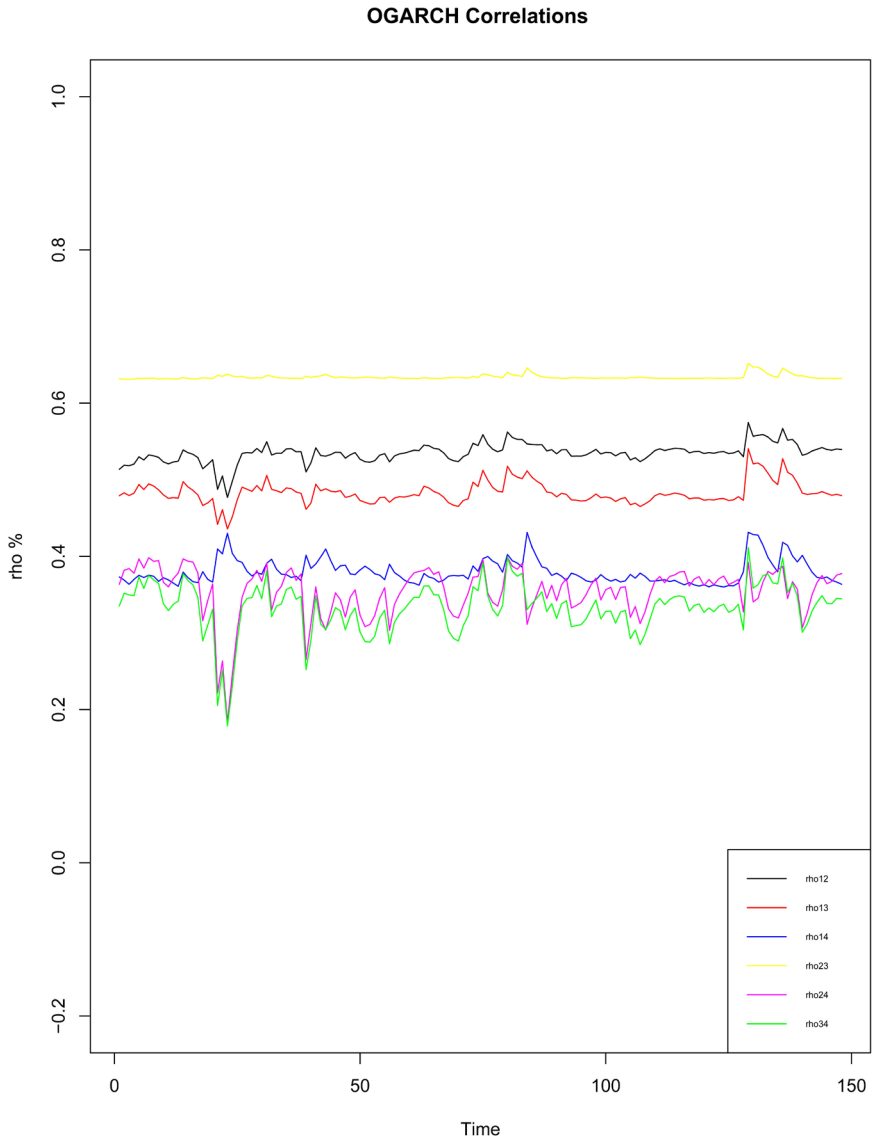


Figure 20. OGARCH portfolio correlations from 2017/06/01 to 2018/01/01.

lags and 12 portfolio observations greater than portfolio VaR. Using one-month window we got 22 lags, and 2 portfolio observations greater than portfolio VaR. We followed the same steps, assumptions and considerations also to calculate VaR and ES in case of normal and Student-t assumption of returns. We obtained the following results:

These values are the numerical result for VaR and ES risk measure concerning the day after the window, that is 2017/12/02, using different methods for different distribution returns' assumptions. Looking at Table 6 and Table 7, we can notice very different values because of different returns' distribution assumption. In particular Table 7 shows that VaR and ES calculated for a month window length are quite high compared to the other windows length. In order to make a decision as to the optimal window size and optimal method we would need to backtest the model.

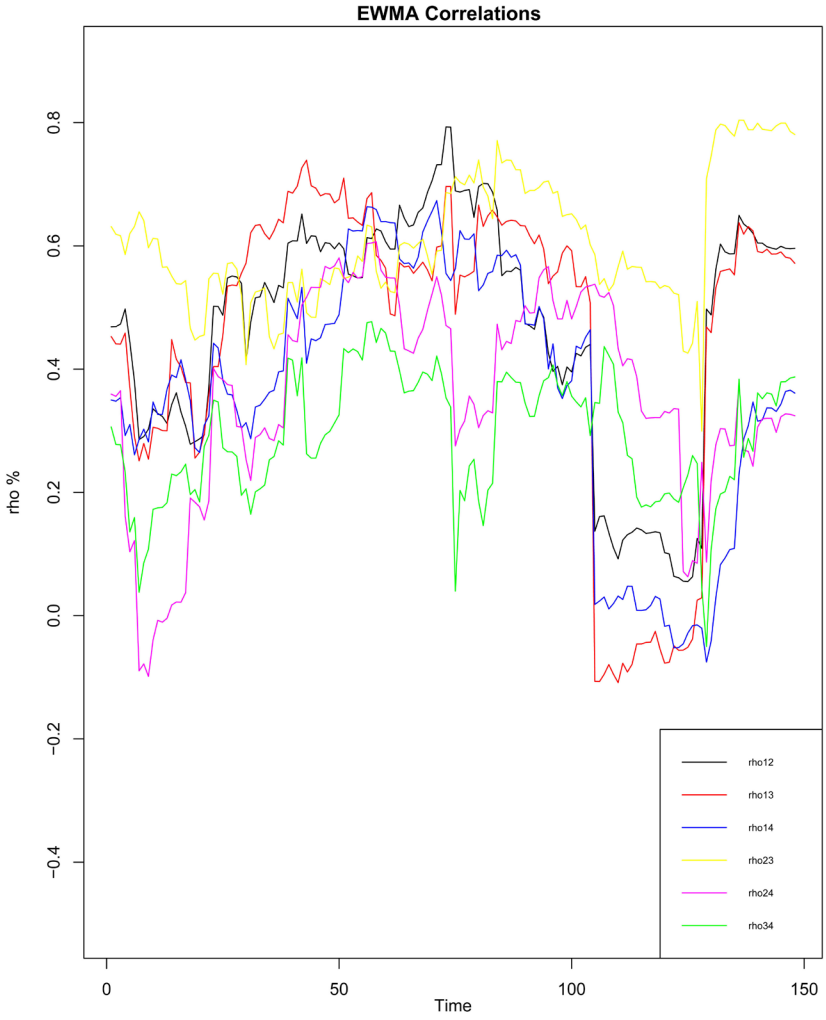


Figure 21. EWMA portfolio correlations from 2017/06/01 to 2018/01/01.

Table 6. HS VaR estimate.

	VAR	ES
2012/01/01-2017/12/01	23.63	34.95
2017/01/01-2017/12/01	14.59	18
2017/11/01-2017/12/01	17.51	17.51

Table 7. Parametric VaR estimate.

	VAR_n	ES_n	VAR_std
2012/01/01-2017/12/01	26.3	33	28.2
2017/01/01-2017/12/01	15.4	19.3	19.3
2017/11/01-2017/12/01	13.4	16.8	15.4

Finally, ES is the best known sub-additive risk measure and is both theoretically and intuitively preferable to VaR. However, severe practical deficiencies prevent its wide-spread use in real world applications. Not only it is estimated with more uncertainty than VaR, but, even more seriously, backtesting ES requires much larger data samples than backtesting VaR.

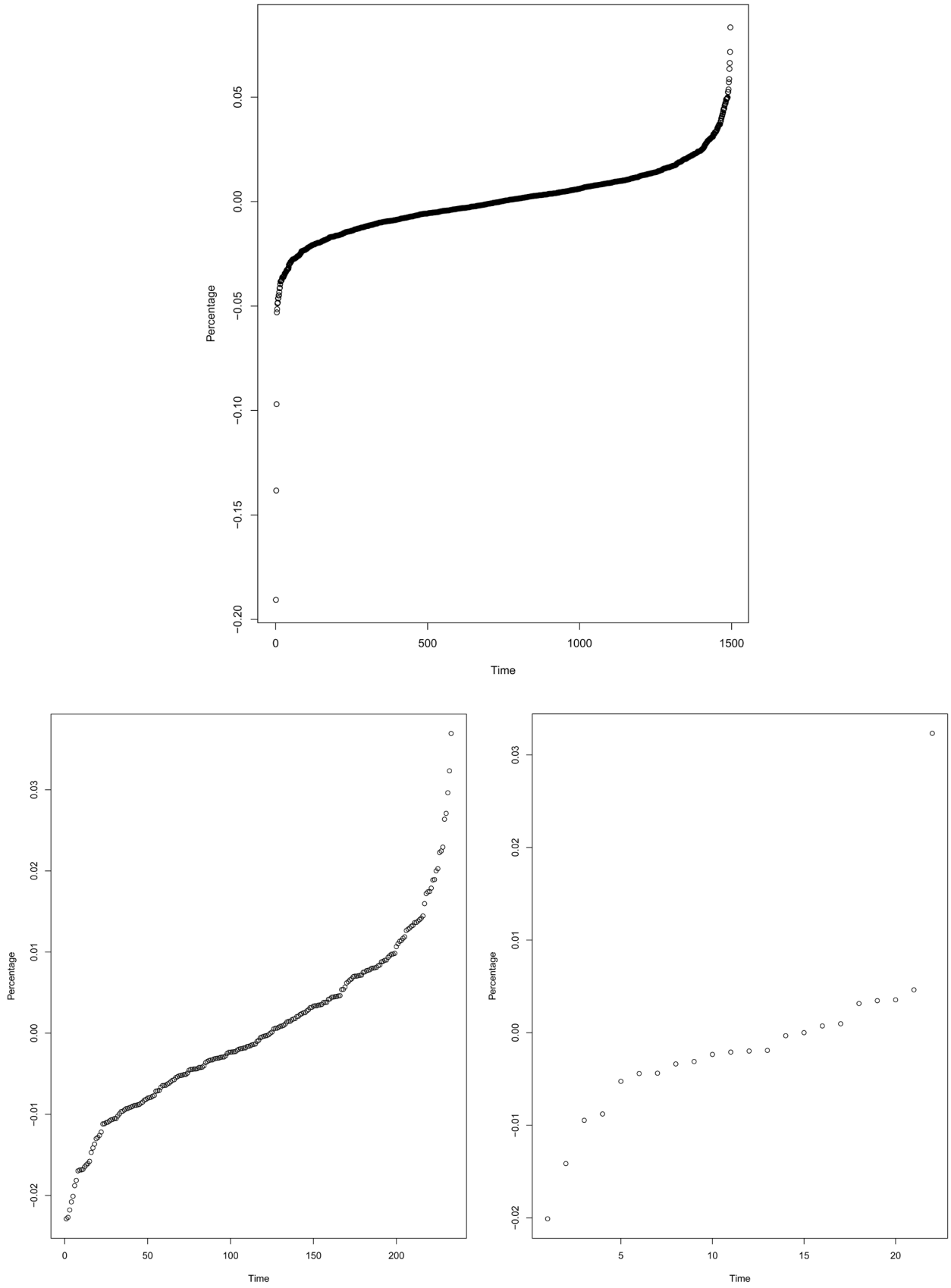


Figure 22. Sorted portfolio returns.

In nonparametric methods (usually, HS) no model is specified and no parameters estimated; however, we have to assume a window length for estimation. The advantage of HS is that it uses observed data directly, is not subject to estimation error and can directly capture nonlinear dependence. The disadvantage is that it is based on fixed weights on returns so that it reacts slowly to structural changes in asset risk. By contrast, parametric methods are based on estimating some distribution of the data, from which a VaR forecast is obtained. This inevitably means that estimation error and model risk become a serious concern, often making the choice of model difficult. There is no single correct choice about which is the best model to forecasting risk. We can diagnose individual models, perhaps by testing for parameter significance or analyzing residuals, but these methods often do not properly address the risk-forecasting property of the models under consideration.

3.7. VaR Backtest

Once we had estimated the VaR and ES for the next day using the various estimation methods, we thought was appropriate to investigate which model worked better than the others using a more or less extensive "WE" time window. Then we calculated the various violation ratios (VR) of each model used and also backtested them through Bernoulli Coverage test and Independence test.

We have firstly to choose the portfolio composition, then we created a matrix with a number of rows equal to the number of lags considered in the time window, while the number of columns considered is equal to 16, *i.e.* four columns for the variances and 12 columns for the covariance. We extracted the initial variance-covariance matrix and inserted the variances and covariance in the first matrix to replace all the 16 columns into matrix 4×4 to have a variance covariance matrix for all the periods considered. We estimated their values for all the rows and columns using the EWMA model. Once we estimated the portfolio variance-covariance for all the periods we evaluated the VaR assuming that the returns were distributed as a normal or as a Student-t.

The second parametric method used to estimate the VaR has been the moving average (MA) using the normal and Student-t returns distribution.

The third method we used to estimate the VaR is the historical simulation (HS), that is a non-parametric method.

Then we plotted all the VaR estimates assuming different estimation window size We = 60, We = 300 and We = 1000.

From Figures 23-25 we can notice how the different models works, in fact EWMA models are more reactive in changing values following better the returns path while MA models and HS react later to return changes, especially if we consider higher estimation window "WE". Obviously in these graphs we considered the entire period WE + WT = 2012/01/01-2017/12/01.

Graphically we can see November 2017 in the last part of the plot in the right; looking accurately it seems that hasn't been too many hits and shock, like

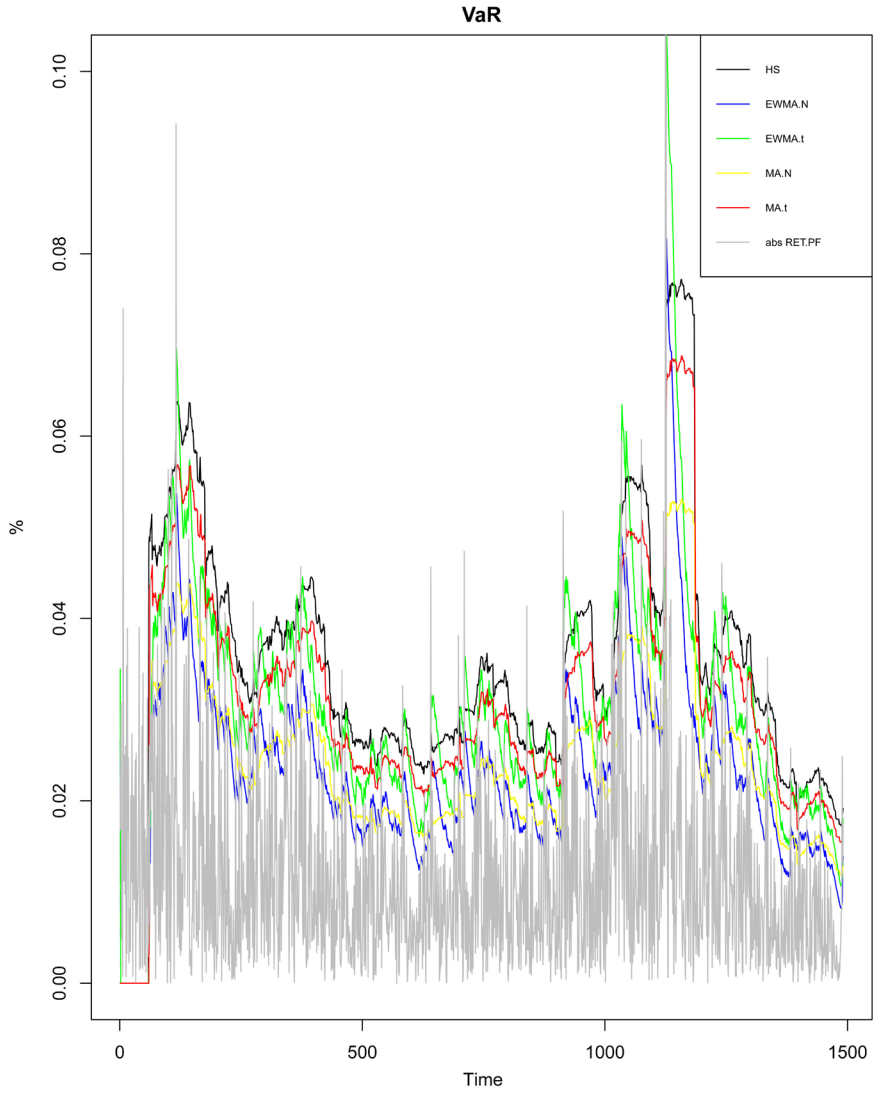


Figure 23. VaR estimates for WE = 60.

2007-2009 crisis, such that the models are not been able to capture the cyber risk shocks.

Going through backtest estimation, first of all we choose the first window length and so we estimate VaR using only past 60 observations for estimate EWMA, MA and HS models. We have to control the hits of November 2017, so in this case we chose an estimation window of 60 lags and a testing window of 30 observations, corresponding on November 2017.

Table 8 shows that HS model is useless because the violation ratio is two, while the other three models are acceptable because MA models and EWMA methods result inside the acceptable window. Considering MA and EWMA models is clear as Violation Ratio (VR) is the same for both methods but considering low VaR volatility the best is the normal one. This portfolio composition, belonging to the financial sector, seems to have a normal returns distribution, because normal VaR works better.

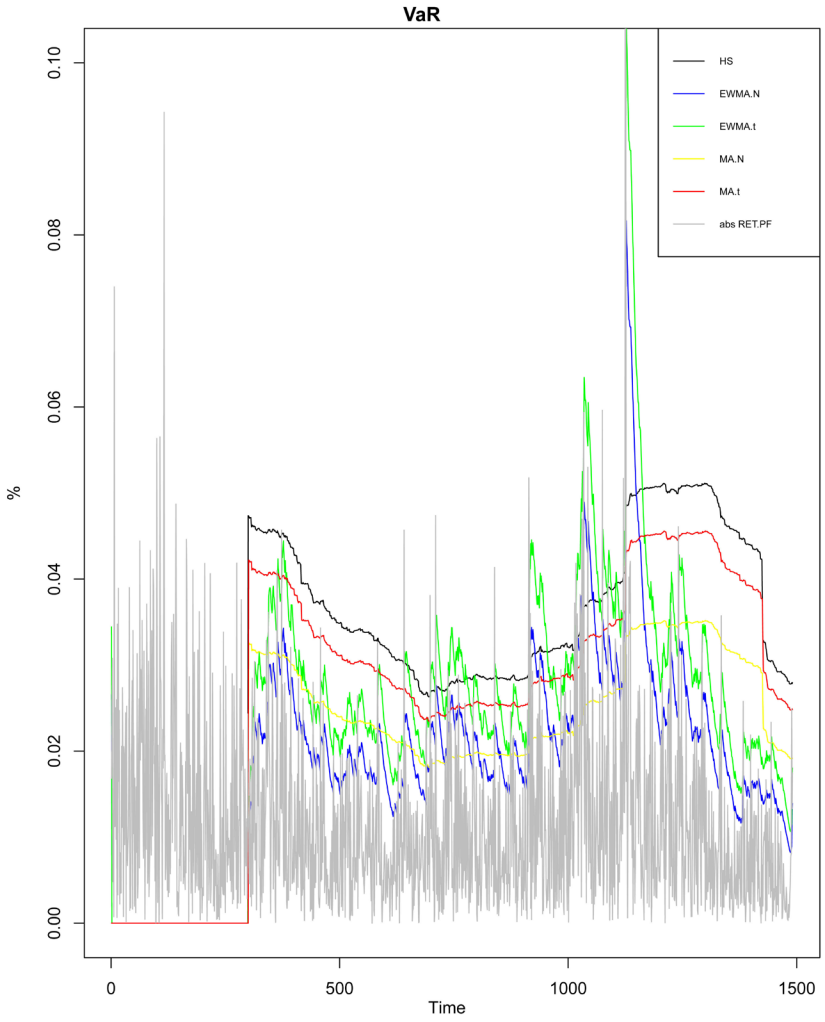


Figure 24. VaR estimates for WE = 300.

Table 8. VR Test for WE = 60 & WT = November 2017.

Method	VR	VaR volatility
EWMA.N	1.333333	0.00177585
EWMA.T	0.666667	0.00217553
HS	2	0.00060324
MA.N	0.666667	0.00074385
MA.T	0.666667	0.00091127

These measures are different if we assume different portfolio weights composition. These values come from the equally weighted portfolio composition, so we suppose to invest 25% of the investment in each portfolio asset.

Figure 26 shows the entire window length WE + WT and one considering only November 2017.

To test the robustness of these results we considered other time windows. The second case we considered is ever an estimation window WE of 60 lags but a bigger testing window WT of 50 lags that correspond to November and December 2017, as shown in Table 9. The series started from 2017/08/08 to 2018/01/01.

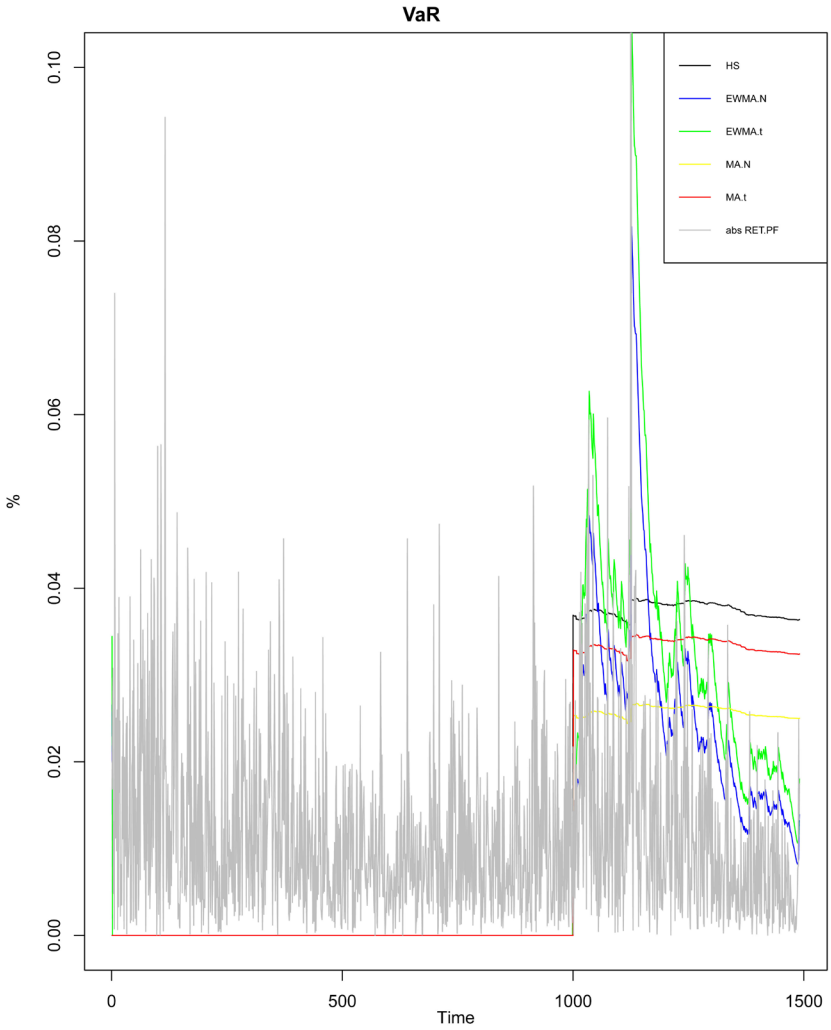


Figure 25. VaR estimates for WE = 1000.

Table 9. VR Test for WE = 60 & WT = November and December 2017.

Method	VR	VaR volatility
EWMA.N	0.833333	0.00267662
EWMA.T	0.416667	0.00327903
HS	1.666667	0.00052920
MA.N	0.416667	0.00066818
MA.T	0.416667	0.00081856

Considering this time window, violation ratio (observed number of violations/expected number of violations) of normal EWMA is the only good model, the other methods are all useless, they stay into the bad window size regarding violation ratio.

The following **Figure 27** is provided for the entire window length WE + WT and the one considering only November and December 2017.

Maintaining WE = 60 we changed another time the testing window considering the period WT = 2017/10/15-2017/12/15.

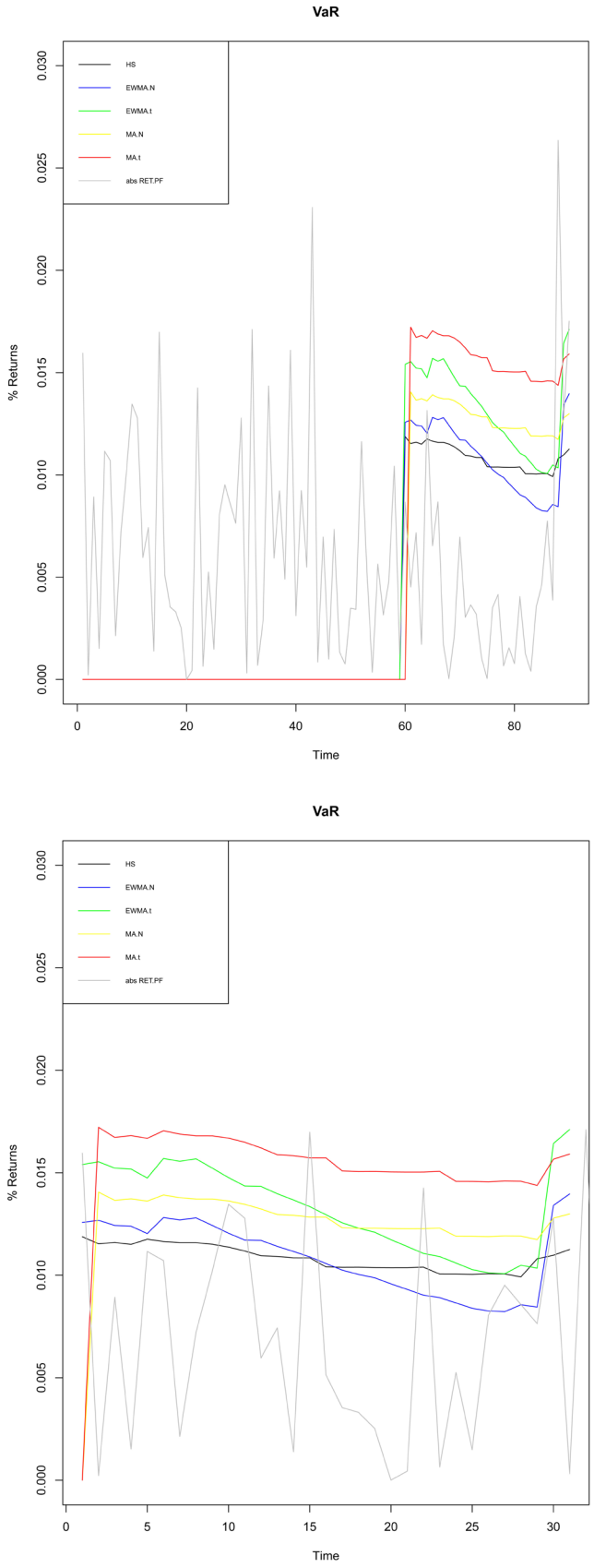


Figure 26. Plotted VaR estimate for WE = 60 & WT = November 2017.

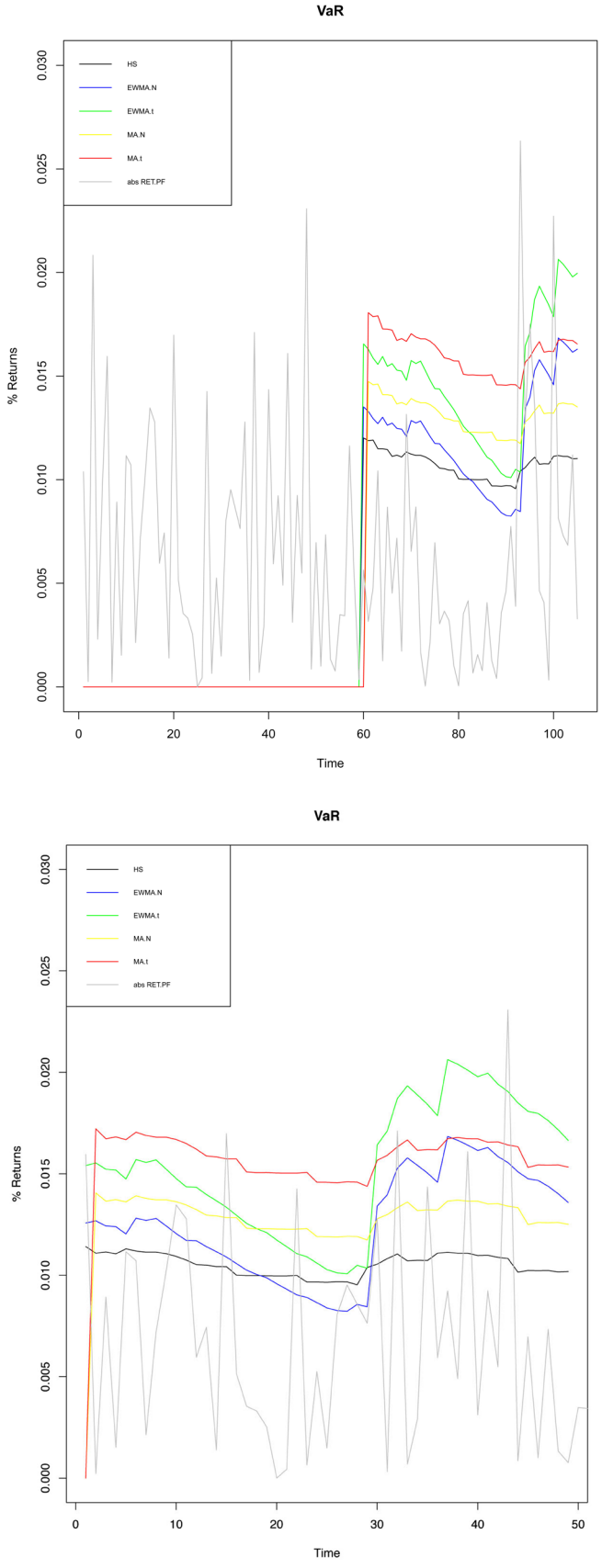


Figure 27. Plotted VaR estimate for WE = 60 & WT = Nov. & Dec. 2017.

Considering the result of this Table 10 we can make the same conclusion done above, EWMA normal seems to be the best method, while the other ones are useless because they belong to bad boundaries thresholds.

Figure 28 provided for the entire window length WE + WT, with WT = 2017/10/15-2017/12/15.

The next estimation window "WE" considered is 2017/06/13-2017/12/01, so in this section we reproduce the same analysis of violation ratios as before but considering WE = 100. Table 11 refers to the estimation window composed by November 2017.

Table 11 shows that all the methods work very well, except HS because it is greater than 1.8. All the other violation ratios are into the best bounds measure, they are all near 1. Looking at the VaR volatility measure normal MA and EWMA methods are the best models because they have the lower value, as presented in Figure 29.

Ever considering We = 100 we focus the attention as before on WT = November and December 17, as reported in Table 12.

Table 10. VR Test for WE = 60 & WT = 2017/10/15-2017/12/15.

Method	VR	VaR volatility
EWMA.N	0.888889	0.00255671
EWMA.T	0.444444	0.00313213
HS	1.777778	0.00063331
MA.N	0.444444	0.00081175
MA.T	0.444444	0.00099444

Table 11. VR Test for WE = 100 & WT = November 2017.

Method	VR	VaR volatility
EWMA.N	0.909091	0.0016765
EWMA.T	0.909091	0.0020539
HS	1.818182	0.0004350
MA.N	0.909091	0.0005287
MA.T	0.909091	0.0006477

Table 12. VR Test for WE = 100 & WT = November and December 2017.

Method	VR	VaR volatility
EWMA.N	0.5	0.0029269
EWMA.T	0.5	0.0035857
HS	1	0.0003389
MA.N	0.5	0.0004216
MA.T	0.5	0.0005165

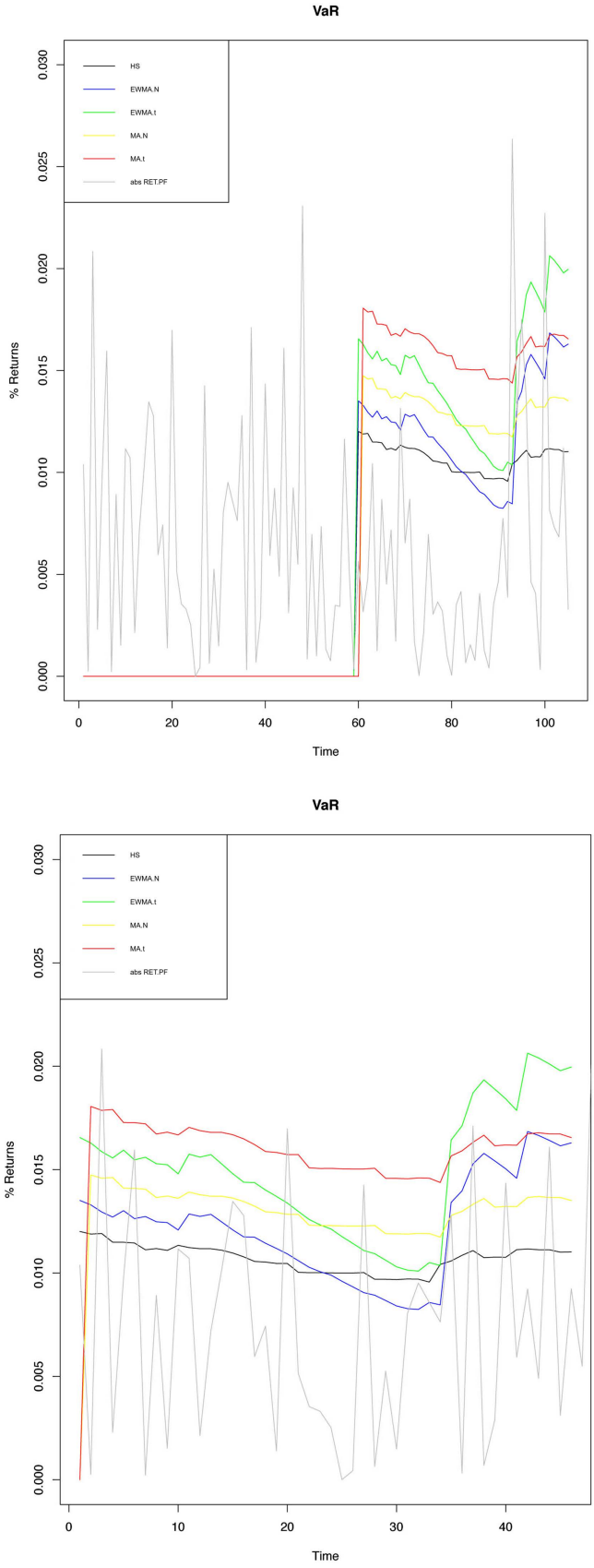


Figure 28. Plotted VaR estimate for WE = 60 & WT = 2017/10/15-2017/12/15.

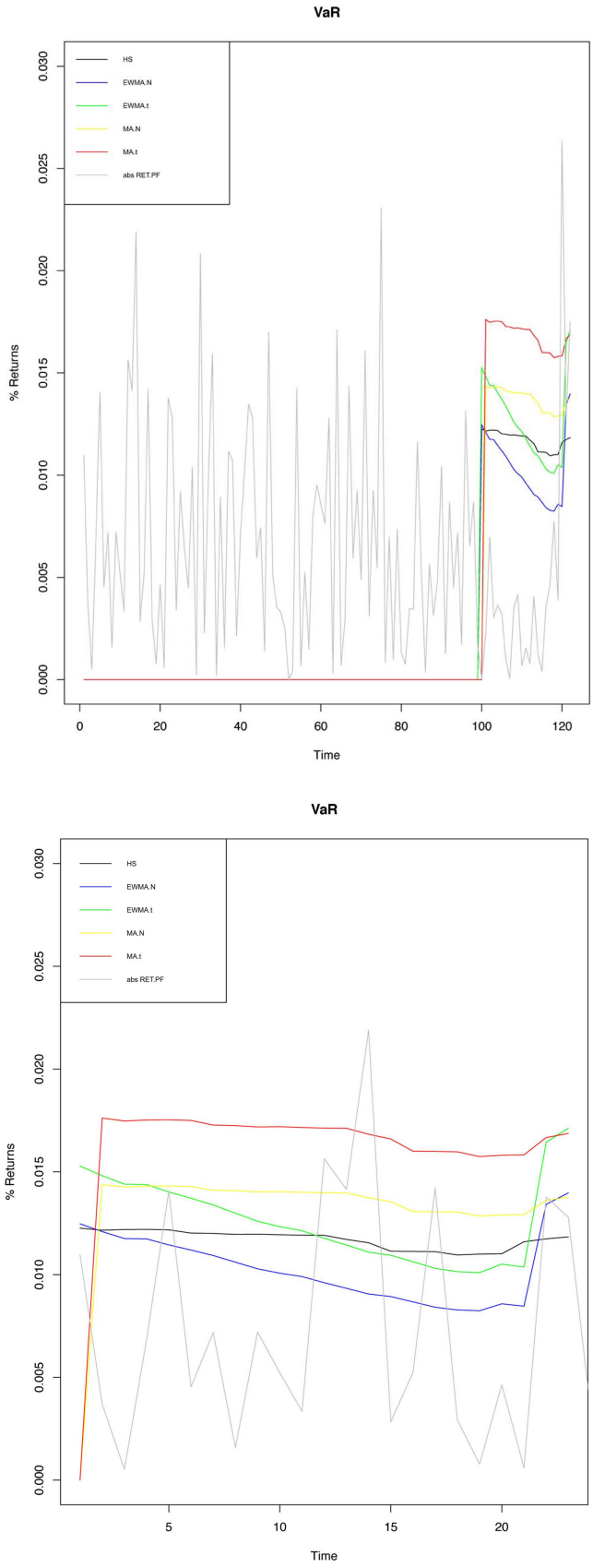


Figure 29. Plotted VaR estimate for WE = 100 & WT = November 2017.

Analyzing the results, in Figure 30, the best model for this estimation window is HS while the others are all acceptable and the best ones are the normal methods.

The last useful consideration is presented in Table 13 where WE = 100 (2017/05/24-2017/10/15) but WT is from 2017/10/15 to 2017/12/15.

The best model is normal EWMA while there is HS method that is acceptable while the others are useless.

Choosing bigger estimation windows becomes useless in order to investigate the impact of a cyber-attack to return series concerning VaR measure, see Figure 31. What seems to be most correct assumption is the fact that models which suppose normality of returns distribution are the measures that work better in terms of violation ratio.

We focus on two issues, the number of violations and clustering, tested by the unconditional coverage and independence tests, respectively.

The unconditional coverage property ensures that the theoretical confidence level "p" matches the empirical probability of violation.

The independence property is subtler, requiring any two observations in the hit sequence to be independent of each other. Intuitively, the fact that a violation has been observed today should not convey any information about the likelihood of observing a violation tomorrow. If VaR violations cluster, we can predict a violation today if there was one yesterday, and therefore the probability of a loss exceeding 5% VaR today is higher than 5%. In this case, a good VaR model would have increased the 5% VaR forecast following a violation.

Unconditional coverage does not impose the independence property and it is possible that a VaR model satisfying one of them would not satisfy the other.

We apply Bernoulli Coverage test and Independence test to the different windows.

3.8. Some Statistical and Financial Results

Concerning time windows considered, the following tables represent the statistic result regarding these two types of test.

Tables 14-16 take the same estimation and testing window used for violation ratio test. In Table 14, WE = 60, WT is November 2017, in Table 15 is November and December 2017, while in Table 16 is 2017/10/15-2017/12/15.

Table 13. VR Test for WE = 100 & WT = 2017/10/15-2017/12/15.

Method	VR	VaR volatility
EWMA.N	0.888889	0.0025567
EWMA.T	0.444444	0.0031322
HS	1.333333	0.0003562
MA.N	0.444444	0.0004383
MA.T	0.444444	0.0005369

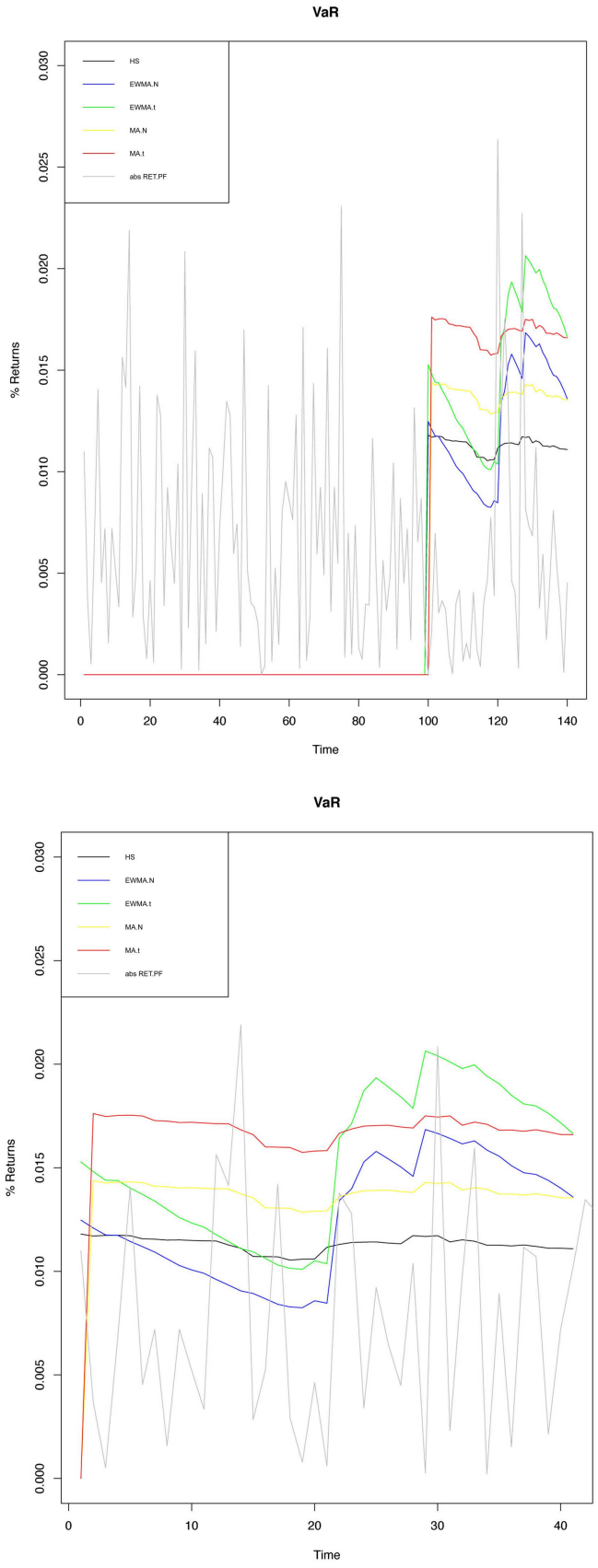


Figure 30. Plotted VaR estimate for WE = 100 & WT = Nov. & Dec. 2017.

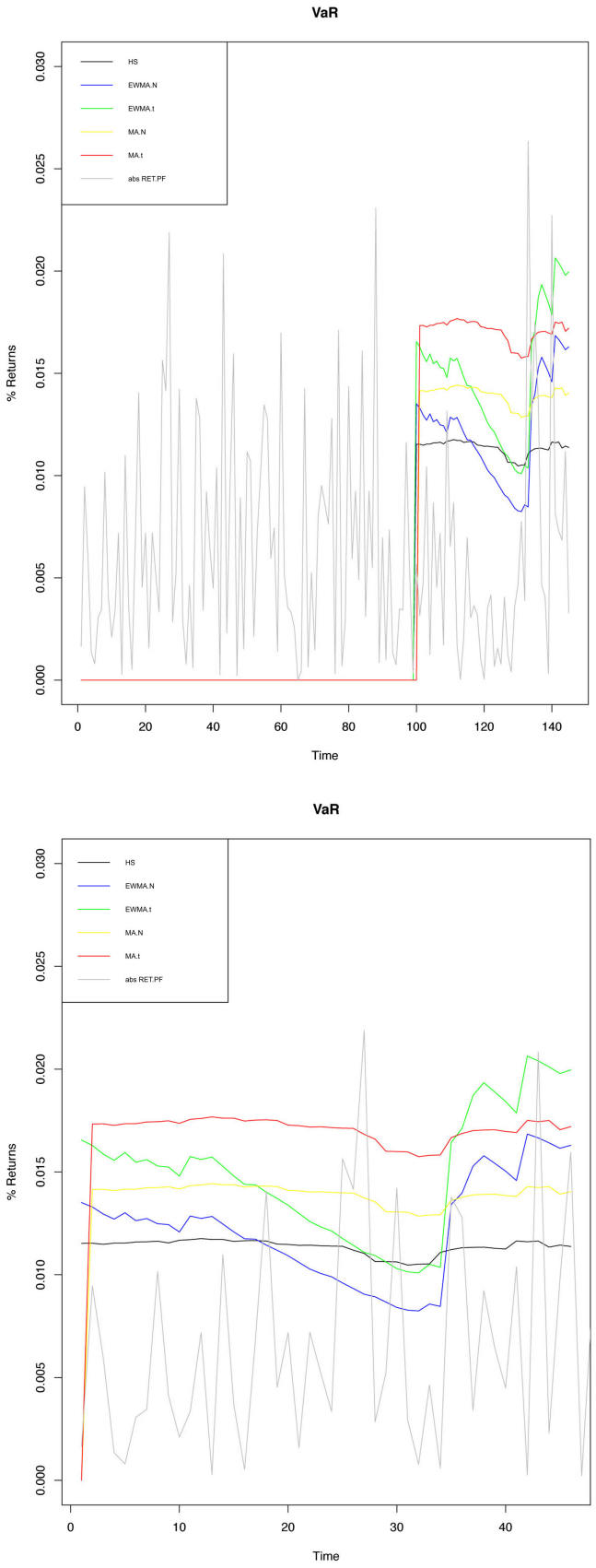


Figure 31. Plotted VaR estimate for WE = 100 & WT = 2017/10/15-2017/12/15.

Table 14. Coverage and independence test WE = 60 & WT = Nov. 2017.

Method	Coverage test		Independent test	
	Test statistic	p-value	Test statistic	p-value
EWMA.N	0.159552	0.689569	0.145535	0.702839
EWMA.T	0.197791	0.656510	0	1
HS	1.239253	0.265615	2.259065	0.132834
MA.N	0.197791	0.656510	0	1
MA.T	0.197791	0.656510	0	1

Table 15. Coverage and independence test WE = 60 & WT = Nov. & Dec. 2017.

Method	Coverage test		Independent test	
	Test statistic	p-value	Test statistic	p-value
EWMA.N	0.074212	0.785299	0.177836	0.673239
EWMA.T	1.091612	0.296114	0.043482	0.834821
HS	0.943414	0.331401	1.100449	0.294168
MA.N	1.091612	0.296114	0.043482	0.834821
MA.T	1.091612	0.296114	0.043482	0.834821

Table 16. Coverage and Independence test WE = 60 & WT = 2017/10/15-2017/12/15.

Method	Coverage test		Independent test	
	Test statistic	p-value	Test statistic	p-value
EWMA.N	0.030327	0.861750	0.190548	0.662461
EWMA.T	0.914338	0.338966	0.046516	0.829241
HS	1.175549	0.278264	0.998538	0.317664
MA.N	0.914338	0.338966	0.046516	0.829241
MA.T	0.914338	0.338966	0.046516	0.829241

Now we consider in Table 17 an estimation window of 100 lags and the same testing window as before: WT = November 2017, in Table 18 is November and December 2017 while in Table 19 is 2017/10/15-2017/12/15.

All the methods implemented have been able to capture the cyber security shocks impact on share returns.

Instead, looking at the violation ratios there are models that work better, especially the normal ones, but is possible to use also the other methods.

Cyber risk is a risk able to give losses to its targets, especially to financial sector firms; but in terms of VaR, managers are able to mitigate losses choosing an adequate VaR method for their portfolio and backtesting that one.

Table 17. Coverage and independence test WE = 100 & WT = Nov. 2017.

Method	Coverage test		Independent test	
	Test statistic	p-value	Test statistic	p-value
EWMA.N	0.009857	0.920913	0	1
EWMA.T	0.009857	0.920913	0	1
HS	0.630673	0.427109	5.268063	0.021720
MA.N	0.009857	0.920913	0	1
MA.T	0.009857	0.920913	0	1

Table 18. Coverage and independence test WE = 100 & WT = Nov. & Dec. 2017.

Method	Coverage test		Independent test	
	Test statistic	p-value	Test statistic	p-value
EWMA.N	0.639794	0.423786	0.526377	0.818535
EWMA.T	0.639794	0.423786	0.526377	0.818535
HS	0	1	3.810143	0.050943
MA.N	0.639794	0.423786	0.526377	0.818535
MA.T	0.639794	0.423786	0.526377	0.818535

Table 19. Coverage and independence test WE = 100 & WT = 2017/10/15-2017/12/15.

Method	Coverage test		Independent test	
	Test statistic	p-value	Test statistic	p-value
EWMA.N	0.030327	0.861750	0.190548	0.662461
EWMA.T	0.914338	0.338966	0.046516	0.829241
HS	0.239328	0.624692	2.102507	0.147058
MA.N	0.914338	0.338966	0.046516	0.829241
MA.T	0.914338	0.338966	0.046516	0.829241

4. Final Remarks

The research focuses on the cyber-attack impact on targeted firms, considering all economic sectors, in particular the financial one using event study methodology.

The impact on stocks returns measured by CARs has given very interesting results, able to highlight insider trading influences which could be interesting to investigate in more detail. Focusing on the sample of cyber-attacks presented above in fact, we find more negative market returns in the event windows before the cyber risk announcements. We found that the average CARs are negative in all event windows, showing that cyber-attack announcements always lead to negative market returns for a company (the market reacts negatively to the announcement of cyber-attack). The extent of negative market returns varies according to the event windows, as well as the statistical significance of mean

CARs, using "Z test". In particular, results show that the symmetric event windows in relation to the announcement, have a high negative mean CAR.

Reducing the range of the event windows, mean CARs show that the significant negative market returns occur on the days prior to and after the announcement of information security breaches. The official announcement of a cyber-attack is often partly anticipated by a few days: the asymmetric event windows give us results that seem to imply that cybercriminals could be implicated in insider trading.

The stock market recognizes the negative business impacts of a cyber-attack so we created a portfolio of assets composed by listed companies of the same financial sector, targeted simultaneously by a cyber-attack, to investigate the reaction to cyber-attacks, in terms of different correlation of returns. Correlations are useful to understand which is the impact of cyber-security investment on investor behavior and even to investigate if there is a higher or lower correlation between the financial entities that undertook different strategies against cyber-attacks. The results show bigger correlations between asset returns of involved banks that suffered cyber-attack in November 2017 respect to correlations that perform both during all months of 2017 and respect to time window 2012-2018. It means that cyber-attacks have been important and influenced market in particular in these last years. The notable very important result is the fact that one of these banks (HSBA) differently shows a lower correlation, during November 2017, with all the other stocks respect to 2012-2018 and all 2017-year time windows. This impressive result achieved by HSBA is due to an announced very big IT investment after many attacks incurred in the past years that have brought the bank to invest in cyber-security.

The importance of an effective risk management analysis is to ensure not only that investments in cybersecurity reflect the considerable and progressively increasing risk, but also to verify if managers' tools are able to statistically capture cyber risk in terms of VaR. The last section of our research is focused on cyber-risk management tools in terms of VaR investigation. The aim has been to take ex-ante value at risk (VaR) forecast using different methods and compare them with ex-post realized returns. We use VaR Violation ratio, Coverage test (Bernoulli test) and Independence test.

Final test results show that we can choose whichever method we prefer because backtesting the model using statistical tools, namely coverage and independence test, is clear that all the methods have been able to predict losses. Thus, concerning these tests, the use of Historical Simulation rather than Moving Average or EWMA methods, although assuming Normal or Student-t distributed stock returns, seems not to have any important relevance because they work very well, both assuming an estimation window and a testing window of different length.

Instead, looking at the violation ratios, there are models that work better, especially those ones which assume normal stock returns, but is possible to use also the other methods.

Results in fact show that the most correct assumption is the fact that models which suppose normality of returns distribution are the most correct and are the measures that work better in terms of violation ratio, considering all different estimation and testing windows. However, violation ratio tests, likewise Coverage and Independence test, work very well because they give consistent results with a ratio's value near one, showing the robustness of VaR measure during the testing window, which coincides with cyber-attacks days.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Garg, A., Curtis, J. and Halper, H. (2003) Quantifying the Financial Impact of IT Security Breaches. *Information Management and Computer Security*, **11**, 74-83. https://doi.org/10.1108/09685220310468646

[2] Ko, M. and Dorantes, C. (2006) The Impact of Information Security Breaches on Financial Performance of the Breached Firms: An Empirical Investigation. *Journal of Information Technology Management*, **17**, 13-22.

[3] Andoh-Badoo, F.K. and Osei-Bryson, K.M. (2007) Exploring the Characteristics of Internet Security Breaches that Impact the Market Value of Breached Firms. *Expert Systems with Applications*, **32**, 703-725. https://doi.org/10.1016/j.eswa.2006.01.020

[4] Ishiguro, M., Tanaka, H., Matsuura, I. and Murase, I. (2007) The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market. Workshop on the Economics of Securing Information Infrastructure (Arlington), 1-12.

[5] Oates, B. (2001) Cyber-Crime: How Technology Makes It Easy and What To Do about It. *Information Systems Security*, **9**, 1-6. https://doi.org/10.1201/1086/43298.9.6.20010102/30989.8

[6] Kannan, A., Rees, J. and Sridhar, S. (2007) Market Reaction to Information Security Breach Announcements: An Empirical Analysis. *International Journal of Electronic Commerce*, **12**, 69-91. https://doi.org/10.2753/JEC1086-4415120103

[7] Odulaja, G.O. and Wada, F. (2012) Assessing Cyber-Crime and Its Impact on e-Banking in Nigeria Using Social Theories. *African Journal of Computing & ICTs*, **4**, 69-82.

[8] Ettredge, M.L. and Richardson, V.J. (2003) Information Transfer among Internet Firms: The Case of Hacker Attacks. *Journal of Information Systems*, **17**, 71-82. https://doi.org/10.2139/ssrn.334460

[9] Hovav, A. and D'arcy, J. (2003) The Impact of Denial-of-Service Attack Announcements on the Market Value of Firm. *Risk Management and Insurance Review*, **6**, 97-121. https://doi.org/10.1046/J.1098-1616.2003.026.x

[10] Kundur, D., Feng, X., Mashayekh, S., Liu, S., Zourntos, T. and Butler-Purry, K.L. (2011) Towards Modelling the Impact of Cyber-Attacks on a Smart Grid. *International Journal of Security and Networks*, **6**, 2-13. https://doi.org/10.1504/IJSN.2011.039629

[11] Eisenstein, E.M. (2008) Identity Theft: An Exploratory Study with Implications for Marketers. *Journal of Business Research*, **61**, 1160-1172. https://doi.org/10.1016/j.jbusres.2007.11.012

[12] Winn, J. and Govern, K. (2009) Identity Theft: Risks and Challenges to Business of Data Compromise. *Journal of Science Technology & Environmental Law*, **28**, 49.

[13] Geers, K. (2010) The Challenge of Cyber-Attack Deterrence. *Computer Law & Security Review*, **26**, 298-303. https://doi.org/10.1016/j.clsr.2010.03.003

[14] Lilienthal, G. and Ahmad, N. (2015) Cyber-Attack as Inevitable Kinetic War. *Computer Law & Security Review*, **31**, 390-400. https://doi.org/10.1016/j.clsr.2015.03.002

[15] Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003a) Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy*, **22**, 461-485. https://doi.org/10.1016/j.jaccpubpol.2003.09.001

[16] Gordon, L.A. and Loeb, M.P. (2002) The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, **5**, 438-457. https://doi.org/10.1145/581271.581274

[17] Dos Santos, B.L., Peffers, K. and Mauer, D.C. (1993) The Impact of Information Technology Investment Announcements on the Market Value of the Firm. *Information Systems Research*, **4**, 1-108. https://doi.org/10.1287/isre.4.1.1

[18] Brockett, P.L., Golden, L.L. and Wolman, W. (2012) Enterprise Cyber Risk Management. In: Emblemsvag, J., Ed., *Risk Management for the Future*: *Theory and Cases*, IntechOpen, London.

[19] Shackelford, S.J. (2012) Should Your Firm Invest in Cyber Risk Insurance? *Business Horizons*, **55**, 349-356. https://doi.org/10.1016/j.bushor.2012.02.004

[20] Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003) Information Security Expenditures and Real Options: A Wait-and-See Approach. *Computer Security Journal*, **19**.

[21] Uma, M. and Padmavathi, G. (2013) A Survey on Various Cyber Attacks and Their Classification. *International Journal of Network Security*, **15**, 390-396. https://pdfs.semanticscholar.org/ba7b/234738e80b027240e9bfd837bfba61c13e17.pdf

[22] Campbell, K., Gordon, L., Loeb, M. and Zhou, L. (2003) The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, **11**, 431-448. https://doi.org/10.3233/JCS-2003-11308

[23] Pettit, R.R. (1972) Dividend Announcements, Security Performance, and Capital Market Efficiency. *The Journal of Finance*, **27**, 993-1007. https://doi.org/10.2307/2978844

[24] Bener, A.B. (2000) Risk Perception, Trust and Credibility: A Case in Internet Banking. University College of London, London.

[25] Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004) The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, **9**, 70-104. https://doi.org/10.1080/10864415.2004.11044320

[26] Arcuri, M.C., Brogi, M. and Gandolfi, G. (2018) The Effect of Cyber-Attacks on Stock Returns. *Corporate Ownership & Control*, **15**, 70-83. https://doi.org/10.22495/cocv15i2art6

[27] Acquisti, A., Friedman, A. and Telang, R. (2006) Is There a Cost to Privacy Breaches? An Event Study. AIS Electronic Library. https://www.semanticscholar.org/paper/Is-There-a-Cost-to-Privacy-Breaches-An-Event-Study-Acquisti-Friedman/05c60011f0b375b45daf422a67ce205f09f9d82b

[28] Gordon, L.A., Loeb, M.P. and Zhou, L. (2011) The Impact of Information Security

Breaches: Has There Been a Downward Shift in Costs. *Journal of Computer Security*, **19**, 33-56. https://doi.org/10.3233/JCS-2009-0398

[29] Cohen, F. (1997) Information System Defences: A Preliminary Classification Scheme. *Computer and Security*, **16**, 94-114. https://doi.org/10.1016/S0167-4048(97)88289-2

[30] Cohen, F. (1997) Information Systems Attacks: A Preliminary Classification Scheme. *Computer and Security*, **16**, 29-46. https://doi.org/10.1016/S0167-4048(97)85785-9

[31] Cohen, F., Phillips, C., Swiler, L.P., Gaylor, T., Leary, P., Rupley, F. and Isler, R. (1998) A Cause and Effect Model of Attacks on Information Systems. *Computer and Security*, **17**, 211-221. https://doi.org/10.1016/S0167-4048(98)80312-X

[32] Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. and Laplante, P. (2011) Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine*, **30**, 28-38. https://doi.org/10.1109/MTS.2011.940293

[33] Gupta, M., Chaturvedi, A.R., Metha, S. and Valeri, L. (2000) The Experimental Analysis of Information Security Management Issue for online Financial Services. In: *Proceedings of the Twenty First International Conference on Information Systems*, Association for Information Systems, Atlanta, GA, 667-675.

[34] Young, D., Lopez, J., Rice, M., Ramsey, B. and McTasney, R. (2016) A Framework for Incorporating Insurance in Critical Infrastructure Cyber Risk Strategies. *International Journal of Critical Infrastructure Protection*, **14**, 43-57. https://doi.org/10.1016/j.ijcip.2016.04.001

[35] Eling, M. and Schnell, W. (2016) What Do We Know about Cyber Risk and Cyber Risk Insurance? *The Journal of Risk Finance*, **17**, 474-491. https://doi.org/10.1108/JRF-09-2016-0122

[36] Taplin, R. (2016) Managing Cyber Risk in the Financial Sector. Lessons from Asia, Europe and the USA. Routledge, London. https://doi.org/10.4324/9781315675930

[37] Bhattachrya, S. and Thakor, A.V. (1993) Contemporary Banking Theory. *Journal of Financial Intermediation*, **3**, 2-50. https://doi.org/10.1006/jfin.1993.1001

[38] Allen, F. and Santomero, A.M. (1997) The Theory of Financial Intermediation. *Journal of Banking and Finance*, **21**, 1461-1485. https://doi.org/10.1016/S0378-4266(97)00032-0

[39] Cummins, J.D., Lewis, C.M. and Wei, R. (2006) The Market Value Impact of Operational Risk Events for U.S. Banks and Insurers. *Journal of Banking and Finance*, **30**, 2605-2634. https://doi.org/10.1016/j.jbankfin.2005.09.015

[40] Gillet, R., Hubner, G. and Plunus, S. (2010) Operational Risk and Reputation in the Financial Industry. *Journal of Banking and Finance*, **34**, 224-235. https://doi.org/10.1016/j.jbankfin.2009.07.020

[41] Pennathur, A.K. (2001) Clicks and Bricks: E-Risk Management for Banks in the Age of the Internet. *Journal of Banking and Finance*, **25**, 2103-2123. https://doi.org/10.1016/S0378-4266(01)00197-2

[42] Cont, R. (2001) Empirical Properties of Asset Returns: Stylized Facts and Statistical Issues. *Quantitative Finance*, **1**, 223-236. https://doi.org/10.1088/1469-7688/1/2/304

[43] Engle, R.F. and Sheppard, K. (2001) Theoretical and Empirical Properties of Dynamic Conditional Correlation Multivariate GARCH. Economics Working Paper Series, University of California at San Diego, San Diego, CA. https://doi.org/10.3386/w8554

[44] Colacito, R., Engle, R.F. and Ghysels, E. (2013) A Component Model for Dynamic Correlations. *Journal of Econometrics*, **164**, 45-59. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1354526

[45] Christoffersen, P.F. (2012) Elements of Financial Risk Management. Elsevier, Amsterdam.

[46] Meulbroek, L.K. (1992) An Empirical Analysis of Illegal Insider Trading. *The Journal of Finance*, **47**, 1661-1699. https://doi.org/10.2307/2328992

[47] Frino, A., Satchell, S., Wong, B. and Zheng, H. (2013) How Much Does an Illegal Insider Trade. *International Review of Finance*, **13**, 241-263. https://doi.org/10.1111/irfi.12006

[48] Brown S.J. and Warner, J.B. (1980) Measuring Security Price Performance. *Journal of Financial Economics*, **8**, 205-258. https://doi.org/10.1016/0304-405X(80)90002-1

[49] Iheagwara, C., Blyth, A. and Singhal, M. (2004) Cost Effective Management Frameworks for Intrusion Detection Systems. *Journal of Computer Security*, **12**, 777-798. https://doi.org/10.3233/JCS-2004-12506

[50] McConnell, J.J. and Muscarella, C.J. (1985) Corporate Capital Expenditure Decisions and the Market Value of the Firm. *Journal of Financial Economics*, **14**, 399-422. https://doi.org/10.1016/0304-405X(85)90006-6

[51] Fama, E.F., Fischer, L., Jensen, M.C. and Roll, R. (1969) The Adjustment of Stock Prices to New Information. *International Economic Review*, **10**, 1-21. https://doi.org/10.2307/2525569

[52] MacKinlay, A.C. (1997) Event Studies in Economics and Finance. *Journal of Economic Literature*, **55**, 13-39. https://pdfs.semanticscholar.org/aac6/83a678a12a3dcd73389aac7289868847ea73.pdf

[53] Boehmer, E., Musumeci, J. and Poulsen, A. (1991) Event-Study Methodology under Conditions of Event-Induced Variance. *Journal of Financial Economics*, **30**, 253-272. https://doi.org/10.1016/0304-405X(91)90032-F

[54] Mikkelson, W.H. and Partch, M.M. (1988) Withdrawn Security Offerings. *Journal of Financial and Quantitative Analysis*, **23**, 119-133. https://doi.org/10.2307/2330876

[55] Elliott, J., Morse, D. and Richardson, G. (1984) The Association between Insider trading and Information Announcements. *The RAND Journal of Economics*, **15**, 521-536.