Estimation and Prediction of the Presence of Hackers in the IoT based on the Kalman Filter

Ghadeer Safaa Majeed* and Muayed Hanoon Salman**
1Baghdad College of Economic Sciences University, Business Administration Department, Baghdad, Iraq
2Imam Al-Kadhum College(IKC), Computer Technology Engineering Department, Baghdad, Iraq

ghadirsafa.85@baghdadcollege.edu.iq
moedh@alkadhum-col.edu.iq

Abstract. In general, the concept of the Internet of Things is to connect different devices to each other over the Internet. With the help of IoT, different applications and devices can interact and talk to each other, even with the humans, via the Internet. Examples include smart refrigerators that connect to the Internet and inform you of the expiration date of foods in the refrigerator. In fact, IoT enables you to remotely manage and control your used objects with the help of Internet infrastructure. However, an important criterion in such networks is security of the information in it. Because if the customers sense that their data will manipulate or hear with a hostile user they will not trust to such network. In this paper, we wants to present new method to intensify the security of the IoT network with use of Kalman Filtering. The Kalman filter has been used as an algorithm to estimate and predict the presence of the hackers and crackers in the network. It is demonstrated that if we equipped our network with such a smart algorithm not only the security of our network will increase but also more users will trust in our network and migrate to it.

Keywords: IoT, Privacy, Estimation and prediction, Kalman filtering.

1. Introduction:

The security attacks try to get the secure data and want to capture the secure information. Some of the popular security attacks are listed below:

1.1. Guessing attacks

The point of a speculating assault is to utilize computational intends to find what the base-secret is. It is an aberrant methodology as in it can work regardless of whether we are not possessing any type of the base-secret. Guaranteeing the base secret may make the speculating more down to earth however, that is the point of an interference assault. This should be possible in pretty much astute ways. The two fundamental ideas of a speculating assault are the beast constrains approach and the word reference approach.
1.2. Brute force

Most OS's utilization a committed record or database where each username and the comparing secret word is put away. In present day systems there isn't the genuine secret key but instead the cryptographic hash of the secret key that is put away with the username. This is to avert anybody, having the capacity to recover the record, to take in all client passwords. Most authentication components along these lines look at the cryptographic hash of the entered secret phrase as opposed to its plain content. An extra security measure taken is to add an arbitrary steady to the secret key before hashing. This is known as a salt and will make the measure of mixes for every secret phrase (two to the intensity of the length of the salt) bigger.

On the off chance that the assailant could recover the secret key document he would have the capacity to relate each username with the cryptographic hash of the clients secret word. Accepting that the client can pick his secret phrase, it would assuredly be something non-arbitrary. The thought in a beast drive assault is straightforward. The aggressor produces each conceivable mix of keyboard contribution up to a specific length and after that hashes the qualities. On the off chance that any of the produced hash-values turn up in the secret word record the assailant has the relating plaintext secret word. For each new hash-value created the entire secret phrase document is looked for a match, along these lines the aggressor needs to experience every conceivable mix just once. Utilizing this procedure the aggressor will largely locate each second client secret word in the wake of attempting half of every single conceivable mix. This is the main assault conceivable on a secret phrase record if the hash work is extremely one-way and if clients pick their passwords at arbitrary. This is obviously not the basic case and consequently there is a quicker and substantially more viable technique, the lexicon assault.

In the events, that the aggressor cannot recover the secret phrase document, he can in any case dispatch this sort of assault if the system has a PC empowered interface and does not block access after a specific number of fizzled login endeavors.

1.3. Dictionary

The thought is to utilize an immense database of normal passwords and words and additionally blends of them and contrast their hash esteems and the ones put away in the secret key document. In the events, that the aggressor finds a match he additionally has the relating secret key. In the events , that the program used to contrast the hash esteems is capable with build every single conceivable blend of strings shorter than an edge esteem we in reality have a savage power assault.

On the off chance that the aggressor cannot recover the secret key document and the system has a PC empowered interface the assailant can in any case utilize this sort of assault. Consider a site, which requires a secret word to be entered in a shape. The assailant could without much of a stretch compose a little program that posts officially rounded out structures to the site utilizing indistinguishable database from above. For this situation the plaintext secret key would be entered and not the hash estimation of the secret key. In the events, that the site does not have any system to cripple a client after a specific number of fizzled endeavors to login, this assault would eventually succeed.

With the equipment accessible on the ordinary work area of today a fruitful word reference assault is only hours away giving a 8-digit secret phrase. The prepared accessibility of projects for this sort of assault is alarming. LC5, John the ripper just to give some examples. As indicated by Schneier (2000)
"On a 400-MHz Quad Pentium II, L0phtcrack can attempt each alphanumeric secret key in 5.5 hours, each alphanumeric secret word with some regular images in 45 hours, and each conceivable keyboard secret word in 480 hours." Now envision that was in 2000 and with work areas in 2004 having processors equipped for more than 1 GHz it does not look great. The expanding rate of processors and consequently the capacity to recover hashed passwords have before long invade the client's capacity to recollections complex passwords.

1.4. Interception attacks

An interception attack rather than a speculating attack is gone for discovering some type of the base-secret straightforwardly. Albeit significant testing frequently must be done to decode the data, on the off chance that it is encoded, the point is to recover the base-secret straightforwardly.

1.5. Sniffing

A sniffing attack is gone for attacking the correspondences line between the remote host and the authentication server. Sniffing is subsequently an interception attack on the correspondences line. It tends to be done in different conduct requiring diverse hardware relying upon the outline of the data bearer. Most PC empowered systems utilize either wired correspondence or air conveyed correspondence. The thought is to introduce yourself or "the sniffer" some place along the utilized correspondence line. The following stage is to associate with this line utilizing different systems. In the events, that the correspondence is over the Internet, the utilization of any PC along the line of correspondence will get the job done or on the off chance, that you approach any center point or switch along that line these can be effectively controlled to send you the data. Air borne correspondence is regularly less demanding to catch since it utilizes broadcasting systems; in any case, it requires some "not all to normal" hardware.

1.6. Man in the middle attack

In a remote login session, the client certifications will be held incidentally on numerous middle of the road stockpiling areas. This can be distinctive kinds of cushions, reserve memory, site pages, transmitter stations et cetera. A man in the center attack is gone for removing that data from the middle of the road stockpiling. Approaching transitional foundation or gaining admittance to this framework for data extraction is designated "a man in the center attack". There is a blend of this attack powers the remote correspondence to go over foundation that the foe is under lock and key or control of. Utilizing forswearing of administration procedures and the learning of the hidden steering protocol this is now and again conceivable.

1.7. Spoofing and masquerading

This is an interception attack with a masterful touch. The thought is to spruce up like somebody or something the client trusts. In the physical world, there are heaps of models, and
the computerized world holds a rich greenery too. Models include: Fake site pages looking like your online bank, sites looking like understood internet business destinations, counterfeit login programs on client terminals and so on. As you may have seen, mocking can be either neighborhood, similar to a phony login program, or remote, similar to organize caricaturing with a phony server.

### 1.8. Attack on the underlying infrastructure

This sort of attack is an interception attack at the host, server or transitional stockpiling gadget. It requires messing with the equipment or the hidden system on which the correspondence or customer/server design is fabricated. Frequently equipment altering is badly arranged and the utilization of pernicious programming to trade off the host or server system is utilized. Remote programming trade off may incorporate disease of the remote system with a Trojan through email or a break in through an endeavor. The manners by which this might be achieved are various however, the standards continue as before.

### 1.9. Denial of service attack

The point of a denial of service attack is to some degree unique in relation to most different attacks. Rather than endeavoring to access the system, or uncover delicate data, this attack centers on rendering the system unusable. Some approaches to accomplish this is to surge the server system with false demands. Another route is to surge the customer with phony reactions. Both these methodologies abuse the usefulness of the Internet’s steering protocol and a few layers in the OSI show and the TCP/IP stack. Denial of service attacks may not just serve to render systems unusable, they are frequently used to constrain either party to change their method for correspondence to something not so much secure but rather more simple to dispatch different attacks upon.

### 2. Common Security Algorithms in IoT:

There are diverse sorts of encryption strategies which are utilized for the encryption of picture and data. The most widely recognized encryption systems are given as takes after:

#### 2.1. RC2

RC2 is a piece cipher with 64-bits square cipher with a variable key size, which go from eight to 128 bits. RC2 is unprotected against a related-key strike utilizing 234 picked plaintexts. RC2 is a square cipher that scrambles data in bits of 64 bits. RC2 is a symmetric piece cipher that tackles 64-bit (eight byte) entireties. It utilizes a variable size key, in any case, 128 piece (16 byte) key would reliably be viewed as phenomenal. It might be utilized as a bit of the great number of modes that DES can be utilized. This count grows a particular message by up to 8 bytes.
2.2. Advanced Encryption Standard (AES)

Two analysts Vincent Rijmen and Joan made AES in 2000. It uses the Rijndael square cipher. Rijndael key and square length can be 128, 192 or 256-bits. In case both the key-length and piece length are 128-piece, Rijndael will perform nine overseeing rounds. If the square or key is 192-piece, it performs 11 overseeing rounds. AES, Advanced Encryption Standard is a symmetric piece cipher that can scramble data squares of 128 bits using symmetric keys 128, 192, or 256. AES encode the data bits of 128 bits in 10, 12 and 14 round ward upon the key size. Creature control strike is the chief proper device known against this calculation. This encryption is shrewd and adaptable. It can be recognized on various stages especially in little gadgets.

2.3. DES

Data Encryption Standard was to be recommended by NIST (National Institute of Standards and Technology).DES is 64 bits key size with 64 bits square size. 3DES is a revive of DES; it is 64 bit square size with 192 bits key size. In this standard, the encryption technique takes after the imperative DES at any rate related three times to widen the encryption level and the standard safe time. 3DES is slower than other square figure frameworks. 56-bit enter is utilized as a touch of DES and 16 cycle of each 48-bit sub keys are encompassed by permuting 56-bit key. Demand of sub keys is turned while unraveling and the indistinct count is utilized. 64-bit piece survey is made utilizing L and R squares of 32-bit.

2.4. Triple DES

It expands the key size of DES by applying the calculation three times in movement with three different keys. The united key size is in this way 168 bits which is 3 times 56, which was past the extent of savage power.

2.5. RC6

RC6 has a piece size of 128 bits and it bolsters key sizes of 128, 192 and 256 bits. It is in a general sense the comparable as RC5 in structure, utilizing data-subordinate turns, and XOR exercises and particular augmentation; certainly, RC6 could be seen as binding two parallel RC5 encryption outlines. Regardless, RC6 uses an additional duplication errand which was absent in RC5 with a specific extreme goal to make the turn reliant on each piece in a word, and not simply the scarcest huge couple of bits.

3. Innovative algorithm

Our proposed system is based on the Kalman filter, and with this algorithm we will be able to extract a model of a person's health and immune system by looking at the patient's health and health records and using it, and the person's current probability information. Estimate and predict the occurrence of specific complications or illnesses (an overview of the different layers
of the proposed system is shown in Figure 2). But before introducing our algorithm, we need to take a brief look at the Kalman filter. One of the best algorithms that has received much attention in recent decades is the issue of statistical filtering. This is of great interest because, this algorithm processes, processes, and extracts a particular pattern or relationship from the system in all available information from the system being tested. This means that statistical filtering even processes system noise. Wiener introduced the subject of filtering and statistical estimation in the 1930s. His approach and criteria were developed by Kalman around 1960. He reduced the error in the model estimated from the system by the covariance matrix in the linear filter. Kalman filter is one of the statistical filters. By applying the Kalman filter, the classification subject reduces to the estimation of the dynamic system state. The development of the Kalman filter for linear and nonlinear experiments is still very serious.

3.1. Specify an optimized linear filter

Formulas Required for Modeling the State Space of a Dynamic System:

\[ \dot{x} = f(x, u, p) + w \]  
\[ z = Hx + v \]

In these formulas there is a linear relationship between state and output. To simplify the noise parameters, w and v are eliminated. Therefore, the dynamical system equation is summarized as follows:

\[ \dot{x} = f(x, u, p) \]  
\[ z = Hx \]

Also, t is the time required to estimate the exact state. If the parameters of a system are measured several times, the obtained values will be almost a Gaussian distribution. Therefore, the best estimate of a system (x):

\[ \hat{x} = \bar{x} = \int_{-\infty}^{+\infty} x P(x|z) dx \]

The following formula specifies the amount of error in such an estimate:

\[ e = \hat{x} - x \]
And the covariance matrix of such a mentioned error:

\[ E = \frac{1}{\sigma^2} \begin{pmatrix} \sigma^2 & \cdots & \sigma^2 \\ \cdots & \cdots & \cdots \\ \sigma^2 & \cdots & \sigma^2 \end{pmatrix} \]

As you can see from the Gaussian distribution, the value of \( x \) represents the maximum probability density function:

\[ P(\tilde{x}) = \max[p(\tilde{x})] \]

Therefore, the best way to determine the optimal estimation of \( x \) is by specifying a value of \( x \) that maximizes the probability density function. For a particular random variable, the standard form of the Gaussian probability density function will be as follows:

\[ P(y) = \frac{1}{\sqrt{2\pi} \sigma} e^{-\frac{(y - \bar{y})^2}{2\sigma^2}} \quad (-\infty \leq y \leq \infty) \]

For an unlimited system with \( n \) different modes we have:

\[ P(\tilde{x}) = \frac{1}{(2\pi)^{n/2} \sigma^n e^{\frac{1}{2}E}} \begin{pmatrix} \sigma^2 & \cdots & \sigma^2 \\ \cdots & \cdots & \cdots \\ \sigma^2 & \cdots & \sigma^2 \end{pmatrix} \]

In the above formula, \( E \) denotes the variance. Therefore, the problem of maximizing \( P(x) \) is under the measured output constraints:

\[ \tilde{z} = Hx \]

\[ \log[p(x)] \] sets the maximum value of \( x \), so we can solve the problem by using the Lagrangian multipliers as follows:
By deriving \( F(x) \) by the way \( x \) we have:

\[
\frac{dF(x)}{dx} = (\hat{x} - x)^T E^{-1} - \lambda^T H
\]

Maximizing means that:

\[
\frac{dF(x)}{dx} = 0 \rightarrow (\hat{x} - x)^T E^{-1} - \lambda^T H = 0
\]

By transposition we will have:

\[
\hat{x} = \hat{x} - \lambda E H^T
\]

Using the measurement function we will have:

\[
\hat{z} = Hx = H(\hat{x} - \lambda E H^T)
\]

\[
\hat{\lambda} = \frac{(H\hat{x} - \hat{z})}{HEH^T}
\]

By pasting (7) into (6) we will have:

\[
\hat{x} = \hat{x} + EH^T [HEH^T]^{-1}(\hat{z} - H\hat{x})
\]

This formula will maximize the value of the probability density function as well as the optimized estimation of the system; also if we enter \((V)\) or measurement noise in formula (4), then the state estimation will be as follows:

\[
\hat{x}' = \hat{x} + EH^T [HEH^T + R]^{-1}(\hat{z} - H\hat{x})
\]

Where in:
To calculate the new covariance matrix by using formula (9) we will have:

$$R = (\hat{V} - V)(\hat{V} - V)^T$$

(10)

To calculate the new covariance matrix by using formula (9) we will have:

$$E = \overline{e e}^T$$

Thus:

$$E' = E - EHT (HT + R)^{-1} HE$$

(11)

By doing some simplification on equations (9) and (11), we get a new parameter called \( k \) that represents interest:

$$k = EHT [HEHT + R]^{-1}$$

(12)

By doing some summaries in (9) and (11), we will have:

$$\hat{x} = \hat{x} + k(z - H\hat{x})$$

(13)

$$E' = E - kHE$$

(14)

As previously mentioned, we will have:

$$\hat{x} = f(x, u, p) + w$$

Optimized estimate for 1 (x):

$$\hat{x} = f(\hat{x}, u, p)$$

(15)
Assuming the process noise has a mean value of zero, the above formula can be expressed as follows:

\[
\hat{\mathbf{x}} = B \hat{\mathbf{x}}
\]  

(16)

B is the coefficient matrix:

\[
B = \frac{\partial f(\hat{\mathbf{x}}, u, p)}{\partial \mathbf{x}}
\]  

(17)

The estimation error of the measurable state is as follows:

\[
\dot{\mathbf{e}} = \hat{\mathbf{x}} - \mathbf{x} = B \hat{\mathbf{x}} - (B \mathbf{x} + w)
\]

Therefore, the time derivation of the error covariance matrix would be as follows:

\[
\dot{E} = \frac{d}{dt}(\mathbf{e} \mathbf{e}^T) = \dot{\mathbf{e}} \mathbf{e}^T + \mathbf{e} \mathbf{e}^T
\]

As a result:

\[
\dot{E} = BE + EB^T + (ww^T)
\]

The process noise covariance matrix will be as follows:

\[
Q = \mathbf{ww}^T
\]  

(18)

The rate of change of the error covariance matrix can be expressed as follows:
\[ \dot{E} = BE + EB^T + Q \quad (19) \]

The above formula (19) is the control equation for the displacement of the covariance matrix with the dimension function over time. By using equations (13), (14), (15) and (19), any estimation problem can be expressed. Equation (13) is used to validate the optimized estimate \((x')\) of the state parameters at a given time. This is accomplished by maximizing the probability density function model and by using the forward estimation of the system \(x'\), as well as the measured current output of \(z\). Using the formula (14), we can determine the error covariance matrix. Equations (15) and (19) update the state and error covariance matrices. Such parameters are used to optimize process and model estimates. The main parameter in order to model a dynamic system is to model it through a series of differential formulas. To do so, the various features and dimensions of that particular system must be known and defined. But in our system (cloud computing), we have no information about the basic parameters and even the architecture of this network. So in the next section, we will only briefly introduce our algorithm.

4. Conclusion:

IoT provides opportunities to integrate directly into the physical world and computer-based systems, such as smart cars, smart refrigerators, and smart homes, which are nowadays referred to in various discussions and conventions. You know, all these devices fall under the IoT. An important factor in such a network is the security of the data in the network. Because if the providers of the network does not provide enough confidence for the users about their data and privacy of their usages, they will not migrate to such networks and do not used the services in it. In this paper, we suggest new smart algorithm for increasing the reliability and security of IoT network with use of Kalman filtering.

References

[1] John J. Lundblad, “Application of the Extended Kalman Filtering Technique to Ship Maneuvering Analysis”, MSC. Thesis, MIT University, USA, 1974.
[2] Ali Farahani Rad, “Cloud Computing and its Implications for Organizational Design and Performance”, MSC. Thesis, MIT University, USA, 2013.
[3] Bo Peng, Bin Cui, Xiaoming Li; “Implementation issues of a cloud computing platform”; Bulletin of the IEEE computer society technical committee on data engineering.
[4] Bruno Guizzelli Batista, Carlos Henrique Gomes Ferreira; “A QoS-driven approach for cloud computing addressing attributes of performance and security”; Future Generation Computer Systems, Volume 68, March 2017, Pages 260-274.
[5] Laurence T. Yang, Gaoyuan Huang, Jun Feng, Li Xu; “Parallel GNFS algorithm integrated with parallel block Wiedemann algorithm for RSA security in cloud”, Information Sciences, Volume 387, May 2017, Pages 254-265.
[6] Carlos André Batista de Carvalho, Rossana Maria de Castro Andrade; “State of the art and challenges of security SLA for cloud computing”, Computers & Electrical Engineering, In Press, Corrected Proof, Available online 3 January 2017.
[7] S. Seyedi, N. J. Navimipour; “Designing an efficient fault tolerance D-latch based on quantum-
dot cellular automata nanotechnology”; Published by Optik Journal, (ISSN: 0030-4026), Vol. 185, PP. 827-837, May 2019. DOI:10.1016/j.ijleo.2019.03.029

[8] Mehdi Darbandi; “Proposing New Intelligent System for Suggesting Better Service Providers in Cloud Computing based on Kalman Filtering”; Published by HCTL International Journal of Technology Innovations and Research, (ISSN: 2321-1814), Vol. 24, Issue 1, PP. 1-9, Mar. 2017, DOI: 10.5281/Zenodo.1034475.

[9] Mehdi Darbandi; “Proposing New Intelligence Algorithm for Suggesting Better Services to Cloud Users based on Kalman Filtering”; Published by Journal of Computer Sciences and Applications (ISSN: 2328-7268), Vol. 5, Issue 1, 2017; PP. 11-16; DOI: 10.12691/JCSA-5-1-2; USA.

[10] Mehdi Darbandi; “Kalman Filtering for Estimation and Prediction Servers with Lower Traffic Loads for Transferring High-Level Processes in Cloud Computing”; Published by HCTL International Journal of Technology Innovations and Research, (ISSN: 2321-1814), Vol. 23, Issue 1, pp. 10-20, Feb. 2017, DOI: 10.5281/Zenodo.345288.

[11] S. Haghgoo, M. Hajiali, A. Khabir, “Prediction and Estimation of Next Demands of Cloud Users based on their Comments in CRM and Previous usages”, International IEEE Conference on Communication, Computing & Internet of Things; Feb. 2018, Chennai. DOI: 10.1109/IC3IoT.2018.8668119.