IOP Conf. Series: Journal of Physics: Conf. Series **1228** (2019) 012025 doi:10.1088/1742-6596/1228/1/012025

Dynamic design and implementation of security intelligence for industry

Sri Krishna Chaitanya Rudraraju[1*] and Samparthi V S Kumar[2]

[1] Assistant Professor, Department of CSE, Sir C R Reddy College of Engineering, Eluru, India.
[2] Assistant Professor, Department of CSE, Sir C R Reddy College of Engineering, Eluru, India.

E-Mail: skc.rudraraju@gmail.com

Abstract: As The development of Internet of Things (IOT) technology became one of the proponents in the industrial revolution 4.0. Digital transformation began to be applied to the entire manufacturing industry, services, transportation and education which have slowly shifted utilizing IOT technology. The industrial revolution 4.0 has an impact on digital transformation and becomes a necessity that can change business patterns such as the ease of data interaction services between industries to customers that are also supported by ease of access and speed of decision making. However, in its development, stakeholders tend to focus on infrastructure and information systems, while the security of information systems is still a comfort zone for industries in the transformation to industry 4.0. The issue of information system security will be a challenge for the industry with open access to information systems; otherwise focus will hamper the business process of the industry. In this research will be discussed about the modeling and implementation of information system security with a combination of web-based security methods with port knocking firewall model and short message service gateway as a security medium with the concept of ease of access with safe and comfortable. The result of this research has been testing penetration testing using network tools.

Index Terms*: *Industry 4.0, cyber security, port knocking, short message service gateway

1. Introduction

The current industrial revolution has grown to 4.0 which replaces industry 3.0. According to [1] and [2] that the basic principle in industry 4.0 is the incorporation of machines, workflows, and systems, by applying intelligent networks along chains and production processes to control each other independently. There are four aspects of the challenges of implementing the industry revolution 4.0 according to Wolter namely information technology security issues, reliability issues and stability of production machinery, lack of adequate skills, lack of motivation of stakeholders to change; and the loss of a lot of work as it turns into automation [3] and [4]. Support of the Internet of Things (IOT) became the most important in the industry revolution 4.0 with open access to information systems and automation changed the way business as its own competitiveness for each industry [5] and [6] According to [7] and [8] security issues will be a challenge for each industry, sometimes for mature industries with adequate resources often overlooking security issues. For medium and small industries some have difficulty and lack of understanding of the security of information systems, stakeholders tend to focus on infrastructure and information systems as digital transformation in the speed of decision making. According to [8] the risks of information system security have an impact, among others, operational risks of Denial-of Service (DDOS) attacks, data theft, website hijacking and reputation risk of lack of trust of business colleagues followed by exposure through media about security vulnerabilities system. In addition, investment risk becomes the most perceived big losses that are large investments but the system is not integrated and the security system used is not in accordance with business needs.

IOT will lead to new problems related to information systems security management, namely the opening of connection lines. This is often used by hackers / hackers to steal data through the network. One of the most important components in an information security management system design is the use of firewalls [9]. The main role and task

of a firewall is to filter and monitor in and out access to application communications connected to the intranet or internet network and communicate the network using TCP and UDP ports that are part of the transport layer of the OSI layer standard [10]. Through the path will appear communication between wide network / internet with internal network and vice versa. Information systems that are in the internal will open a certain communication path and can be reached.

From this background phenomenon in this research try to do design development of information system security with IOT support with model combination 2 authentication user / password and short message. The device used from the security model uses Raspberry PI devices, mikrotik Router as Firewall and SHORT MESSAGE gateway. The purpose of this research is as a model solution for the security of information systems with easy technical operation but with a high level of security and comfort with safe and convenient operation techniques.

2. Review of Literature

2.1 Computer Network

A computer network is a system of computers designed to share resources, communicate and access information. The purpose of a computer network is to be able to achieve its purpose, any part of the computer network can request and provide services. Computer networks can also be interpreted as a collection of communication terminals located in various locations consisting of more than one interconnected computer. The purpose of building a computer network is to carry information precisely without any error from the transmitter side to the receiver side through communication media [3]; [4] and [5]. Computer networks can also be defined as a collection of different communication terminals in different locations consisting of more than one interconnected computer [7]

Two computers each have a network card, then connected via cable or wireless as a data transmission medium, and there are network operating system software will form a simple computer network. If you want to create a wider network of computers again reach, it requires additional equipment such as Hub, Bridge, Switch, Router, Gateway as interconnection equipment.

Based on the scalability of computer network classification is as follows [5]:Local Area Network (LAN) is a network that is used for personal, whether within a building or in one campus area. Reach which can be reached by LAN up to several kilometers. LAN is used to connect private end devices to exchange data.

Metropolitan Area Network (MAN) is a network widely used to connect nodes located at a distance of 20-50 Km, this network is commonly used for inter-city by using radio pocket or telecommunication company facilities [11].

Wide Area Network (WAN) is a network of data communication systems that each node is located remote (remote location) with each other. WAN is also called the remote network / long distance network. A node is a point that can receive input data into a network or produce output information or both. Node can be either a printer or other print tool or a PC to a computer mainframe that has a modem [12].

2.2 Security Management Using Web Knocking Port Technique

Knocking port is a technique or method of opening ports externally through a firewall by way of attempting to connect to a closed port with a predetermined connection attempt sequence [6]; [8] & [10]. In other words port knocking is a method for building a host-to-host communication with a computer device that does not open any communication ports freely.

The Web Knocking port is implemented by configuring a small program called a daemon to monitor the firewall log for connection requests and determining whether the client is registered on an approved IP address and has done the correct sequence. If the answer is yes, the firewall will open the associated ports dynamically.The main purpose of knocking ports is to prevent attackers from system scanners such as remote access SSH by doing port scanning [6] and [11]. If an attacker sends an incorrect sequence of beats, the protected port will not appear or open as shown in Figure 1and Figure 2.

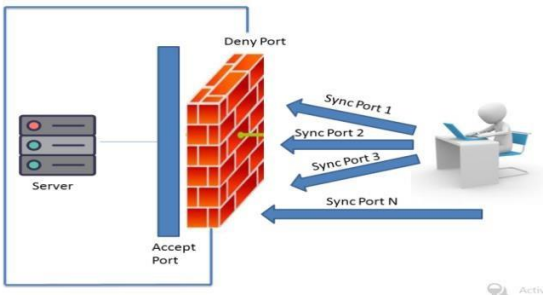

Figure 1: Knocking Port

2.3 Firewall Security Management

A firewall is a security system designed to prevent access or attacks from within and outside the network. Firewalls can be implemented in hardware and software, or a combination of both. Firewall implementations are generally used to control the access of users accessing private networks connected to the Internet, especially intranets. All incoming or outgoing activity traffic through the intranet network through the firewall will be controlled for users who do not meet certain security criteria will automatically be blocked [7] and [10].

The firewalls function as a controller, watching the flow of data packets flowing in the network. The firewall function organizes, filters and controls the data traffic that is allowed to access private networks that are protected, some criteria that the firewall does include: (a) the IP address of the home computer,(b) TCP / UDP port of origin to destination computer (c) IP address of destination computer TCP / UDP port destination data on destination computer Header information stored in data packet [9].

Specifically the firewall function is to authenticate the network access Figure 2.2 is a firewall implementation image

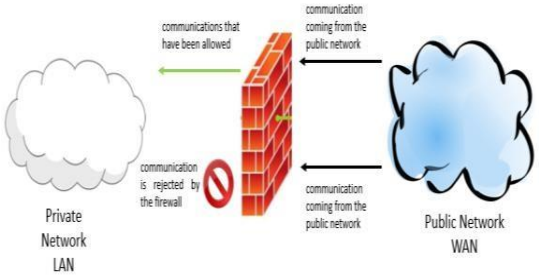

Figure 2: Firewall

How the firewall works in general to protect the internal computer network, among others:

Reject and block data packets that come based on unwanted sources and purpose [10].

Refuse and filter the data packets coming from interstitial network to the internet. His example when there are users of the internet network will access porn sites.

Reject and filter data packets based on unwanted content. For example, an integrated firewall on an antivirus will filter and prevent files that have been infected with a virus trying to enter the internal network. Report all network activity and firewall activities.

2.4 Short Message Gateway

Short message gateway is an application system that serves short messagesubmissions and receipts, widely used in business applications, both for the purpose of broadcast promotion, information services to users and dissemination of product or service content and so forth. Short message gateway is also an application, in which there is a SHORT MESSAGE feature that can be modified as needed. For example some of the features commonly developed in short messageservice apps

The gateway is a mass-shipping automated or scheduled tail cast message [3]. In addition, it plays an important role in sending short messageservice gateway called short message service center which is a mobile phone network that handles the sending of short message service center. So, when someone sends short message service center message through their mobile phone, the short message service center in charge sends the message to the destination number. If the destination number is not active, the short message service centerwill retain the message within a certain period of time. If the short message service still cannot be sent until the time period expires, then the short message service will be deleted from the short message service center storage. Gateway application can use the short message service centerpath for its operation.

2.5 Database

A database is a collection or complete operational data set of an organization that is organized or managed and stored in an integrated manner by using certain methods using a computer so as to provide the optimal information that the user needs [12]. While the database system is a system of arranging and managing records using computers to store or record and maintain complete operational data of an organization or company so as to provide optimal information that the user needs for the decision-making process [11].

According [11] and [13] Understanding Database is: "Collection of files that have links between one file with another file to form a data building to inform an agency company, within certain limits". The above conclusion is the database is a collection of data interconnected with each other, stored in a computer and used software to manipulate it.

2.6 PHP Programming Language

PHP is one of the scripting languages installed in HTML. Most of the syntax is similar to C, Java and Perl, plus some specific PHP functions. The main purpose of this language is to enable the web designer to write dynamic web pages quickly. PHP was written and first introduced around 1994 by Rasmus Lerdorf through his website to find out who has accessed his online summary [14].

PHP is a script-shaped language that is placed in the server and processed on the server PHP is a script-shaped language that is placed in the server and processed on the server. The result will be sent to the client, where the userusing the browser. PHP is known as a scripting language, which integrates with HTML tags, is executed on the server, and is used to create dynamic web pages as well as Active Server Pages (ASP) or Java Server Pages (JSP). PHP is open source software. In particular, PHP is designed to form dynamic web. That is, it can form a view based on current demand. In principle, PHP has the same functionality as scripts such as ASP (Active Server Page), Cold Fusion, and Perl [14].

2.7 MikroTiks

Mikrotik is a small company headquartered in Latvia, adjacent to Russia, its formation initiated by John Trully and ArnisRiekstins. American John Trully immigrated to Latvia and met Arnis with Physics and Mechanics scholarship around 1995. In 1996 John and Arnis began to rout the world (Mikrotik's vision is to routing the whole world). Starting with Linux and MS DOS systems combined with the 2Mbps Aeronet Wireless LAN (W-LAN) technology in Moldova, Latvia's neighbor, and then serving five of its customers in Latvia, because their ambition is to create one reliable and deployed router software across world.

This is somewhat contradicted by the information that is on the web Mikrotik, that they have 600 point (customer) wireless and largest in the world [7]. Mikrotik is a computer network device in the form of Hardware and Software that can function as a Router, as a tool Filtering, Switching and others. The Mikrotik hardware can be a PC Router (which is installed on the PC) or a Router Board (already built directly from the company Mikrotik). While mikrotik software has known as RouterOS there are several versions. One of the well-known versions of RouterOS today is RB1100 [7]. One example of Router Board hardware can be seen in

Figure3:MikrotikRB450G [8]

Their basic principle is not to make Wireless ISP (WISP), but to make the router program that is reliable and can run all over the world. Latvia is simply the "place of experimentation" of John and Arnis, because now they have helped other countries including Sri Lanka serving about four hundreds of its customers.

2.8 Types of Mikrotik

Mikrotik has 2 products such as mikrotik OS and MikrotikRouterboard.

1. MikroTik RouterOS is an operating system and software that can be used to make the computer become a reliable network router, covering various features made for ip network and wireless network, suitable for use by ISP and hotspot provider. For the installation of mikrotik is not required additional software or other additional components. Mikrotik is designed to be easy to use and very well used for the purposes of computer network administration such as designing and building a small to complex computer network system though.
2. MikrotikRouter Board is an embedded router product from mikrotik.

Router board is like an integrated mini pc because in one board embedded processor, ram, rom, and flash memory. Router board using RouterOS that serves as a network router,bandwidth management, proxy server, dhcp, dns server. All of them can also function as a hotspot server.

2.9 Mikrotik Function

The main function is to make a computer mikrotik as a network router (Routing). In addition, mikrotik also has a function to run applications, including: Application Bandwidth Access capacity, Application Firewall, Wireless Access Point (Wi-Fi), Backhaul Link Application, System Hotspotand Virtual Private Network (VPN) Server

Router

Router is a computer network device that can serve to forward packets of data from one network to another network that is different in a computer network [7]. This router can be built using mikrotik. 3.3. GNS3 GNS3 is a graphical network simulator program that can simulate a more complex network topology compared to other simulators. This program can run on various operating systems, such as Windows, Linux, or Mac OS X [9].

Firewall

A firewall is a device that is placed between the Internet and the internal network. Information coming out or incoming must go through this firewall. A Firewall is a software (Software) or hardware (Hardware) that filters out all traffic data (traffic) between our computers, home or office computer networks with the Internet. Firewall in a network, will ensure that when things go wrong bad on one side of the firewall (such as the Internet) then the computer on the other side will not be affected.

The basic function of a firewall is

1. Packet Filtering: All headers of data packets passing through the firewall will be checked, here the firewall makes a clear decision to allow or block each packet.
2. Application Proxy: Firewall is able to check more than just the header of a data packet, this capability requires the firewall to be able to detect specific application specific protocols.
3. Monitoring and recording traffic: Keeping track of what's happening in the firewall is very important, so it can help us to estimate the possibility of a security crashing or provide useful feedback about firewall performance.

Virtual Private Network (VPN)

VPN (Virtual Private Network) is a private network that connects one network node to another network node using the Internet network. The data passed will be encapsulated and encrypted, so that the data is guaranteed confidentiality. A VPN is a facility that allows remote connections using a public network for access to a Local Area Network (LAN) in an enterprise. VPN is a way to make a network private and secure by using public network such as Internet. VPNs can send data between two computers that pass through the public network so as if connected point-to-point. The data is encapsulated with a header containing the routing information to obtain a point-to-point connection so that it can pass through the public network and can reach its final destination.

VPN Development

VPN was developed to build an intranet with a broad reach through the Internet network. Intranet has become an important component in a company today. Intranet within the company can grow in accordance with the development of the company. In other words, the bigger a company should have wide bandwidth of the intranet. So the problem becomes more complex if a company has a branch office with a long distance. While on the other hand

is always related, for example sending a data and data synchronization [4]. The rapid development of the Internet offers a solution for building an Intranet using a public network or the Internet. On the other hand, an industrial development also demands five needs within the Intranet: (a). Confidentiality, i.e. the ability to encrypt messages along unsafe networks. (b). Access control, which determines who is granted access to the network and what information and many people can accept. (c). Authentication, which examines the identity of two companies that make transactions (d). Integrity, i.e. ensuring that files do not change in transit. (e). Non-repudiation, i.e. preventing two companies from denying.

Raspberry Pi

Beginning with concerns over the decline in skills and the number of students wanting to study computer science, Eben Upton, Rob Mullins, Jack Lang and Alan Mycroft from the Computer Laboratory of Cambridge University, England, together with Pete Lomas and David Braben in 2009 founded a nonprofit foundation named Raspberry Pi Foundation. The main purpose of this foundation is to promote the basic learning of computer science in schools.

The name Raspberry Pi itself, then pinned on a credit card-sized minicomputer, was first released to the public in February 2012. Raspberry Pi, or often shortened to Raspy, is the type of Single Board Computer (SBC) the size of a credit card developed by the Raspberry Pi foundation, with a view to learning basic computer science at school. Raspberry Pi and Raspberry Pi 2, manufactured by several electronics manufacturing companies namely; Newark element14 (Premier Farnell), RS Components and Egoman. The hardware produced by some companies is the same with each other. Especially Egoman, this company produces for marketing in Tionghoa (China) and Taiwan. Egoman version can be distinguished on the color of his board is red.

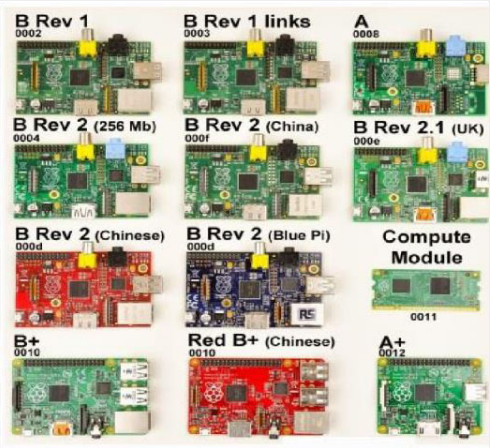

Figure 4: Type ofRaspberry Pi

Raspberry Pi does not have a RTC (Real-Time Clock), so Raspi cannot save time when resources are turned off. Alternatively, we can create a script that runs during the first boot process to get the time from the NTP (Network Time Protocol) server. We can also add IC (Integrated Circuit) RTC like DS1307 with backup battery through I²C channel (Inter-Integrated Circuit) in GPIO (General Purpose Input / Output).

2.10 Port Knocking

Port-knocking is the concept of hiding a remote service inside a firewall that allows access to the port only to know the service after the client has been successfully authenticated to the firewall. This can help to prevent the scanner from knowing what services are currently available on the host and also serves as a defense against zero-day attacks [4]. 3.5. Hacking is an intrusion activity into a computer or network system in order to abuse or damage existing systems. The definition of the word "misuse" has a very broad meaning, and can be interpreted as theft of confidential data, as well as inappropriate use of e-mail such as spamming or searching for possible network gaps to enter [10]. Inside the firewall all incoming and outgoing communications are controlled. Unnecessary ports can be blocked (closed) and important and dangerous ports can also be blocked, so only allowed parties can log in through that port. This is the most effective and widely used computer network security system. But sometimes blocking is often inflexible, when needed to establish communications with what's inside the network, firewalls do not allow it because it might be in an unauthorized area.Firewallsthough are a toolcommunication [11]. Itto be done is very important for

the smooth work. For example connecting to the internet and needing to access the web server via SSH to fix the configuration, while the SSH port on the server is prohibited to be accessed from the internet by the firewall, of course this will be very inconvenient. To avoid this sort of thing, there is a very effective method that is by using port knocking method. Port knocking is a method for building communication between computers from anywhere as long as each computer is connected in a computer network, with a computer device that does not open any communication port freely, but the device is still accessible from outside, using a configuration format an experimental tap port to transmit connections on the tap port.

2.10.1 Benefit of Port Knocking

Port Knocking is a great method as a way of connecting to their computer devices. Port knocking is suitable for those who still want to strengthen their computer security system and network devices, while still wanting to have a personal connection to it continuously and can be done from anywhere. Personal communication means a connection that is not open to the public like SMTP or HTTP. Usually this personal communication is more administrative and uses services such as telnet, SSH, FTP, TFTP, and more. This personal communication will be very dangerous if it can also be done by others who are not eligible. By using Port knocking, these services will remain closed for public access, but can still be flexibly opened by anyone who has a combination of tap ports.

2.10.2 Port Knocking Implementation

Implementation or implementation of the knocking port can be implemented on several devices or operating systems that provide features or service firewall for example Linux and UNIX based operating system [9] and [10]. Port knocking on its basis can be implemented by custom-rule firewall rules that exist in each device or Operating system. Implementation of port knocking on Linux or UNIX based operating system, because in addition to open source firewall rules in the operating system can be modified in such a way that the use of firewall to be more effective in accordance with the interests.

3. Research Method

Stages in this research begin from the identification of needs, literature studies, design of information systems security management, VPN system development, testing, and implementation as Figure 5

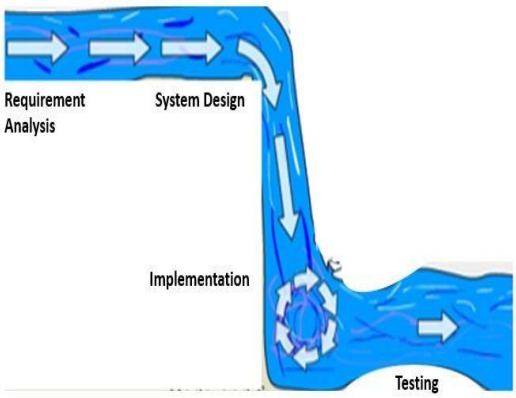

Figure 5: Research Design

Stages performed in the study are:

3.1 Requirement Analysis

At this stage the identification of problems to be solved based on the theory and practice of the application. Besides that, there is also a need analysis of system development, both from network aspect and its security as well as application development aspect. This identification needs to be done so that details of the development of information system security model can be tailored to the needs of its users.

3.2 System Design

Some of the literature referred to in this study discuss about network management, network connection, network security, user database, and programming is used to support the development of web knocking model in this research. References used from some similar research that has been done by other researchers also become an important reference in overcoming trouble shooting during development.

3.3 Implementation

The model will be based on the results of problem identification and needs analysis. The design of information systems security management tailored to the needs of users. Besides, the components and parameters that will be applied into the system both hardware and software are made in detail by considering the aspects of network security and user convenience. Models that have been made will be used as a reference in the manufacture of network security systems and web knocking based application system. Information system security management is based on the design of web knocking model that has been made in the previous stage. This security system must be able to ward off attacks by the parties who are not responsible (hackers). The enormous risk must be borne by the server owner and the admin system if an open network connection built can be attacked by a hacker. One of the risks is that hackers can retrieve / delete existing data on the server.

All connections to the server either through the local network (LAN) or via the Internet (WAN) network must be guaranteed security. Protection of server network security (firewall) can be done in layered. There are many ways to perform network security. In this research, network security model used is using knocking port. This server knock method is very well used to secure access to the server via a wide network (internet) because only registered users can login into the server. If the user is not recognized and tap the door is not allowed by the admin system, then the user cannot access the system information and if doing some login error it will be identified as hacker / hacker.

After system development on the network, the next step is to build a web-based application. The applications used for security connections are of some sort and usually the app is not user friendly. Development of web-based applications will facilitate the user when logged into the network system, which is just by typing a web address. After the user is allowed to enter through the process of entering account (login) in which will do knock the door firewall (knocking) automatically. After successful knocking identification is done, the server sends the token ID via short message service and asks the user to enter the token ID code on the web.

3.4 Testing

After the process of developing the network security system and application login system, the next step is to test. This process requires precision and accuracy by including various possibilities. This is done so that the weakness of the system (hole) that allows hackers to attack can be identified and can be repaired. The smallest possibility should be taken into account considering the open network created allows everyone to try to enter into the built system. The final stage is implementation and documentation. Implementation can be done in the form of socialization to the leaders, lecturers and employees who want access server STIE Perbanas Surabaya by using internet connection from home respectively.

3.5 Overview of Research Model

In Figure 6 an overview of the research model. Stages performed by users who will connect access system information using the Internet network with the condition of the system information server for port 80 (http) is still closed by the firewall, which is begun by logging access through the internet through the browser with web knocking techniques in it. After successful login the user will receive the token ID either via short message or email, the user will enter the token ID on the web. If successful then the Laptop / PC users can access the information system previously port 80 (http) and https (443) closed that can not be accessed through public.

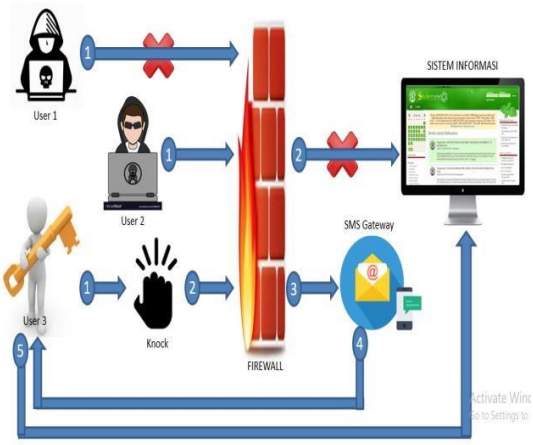

Figure.6: Systems Flow Security Intelligent

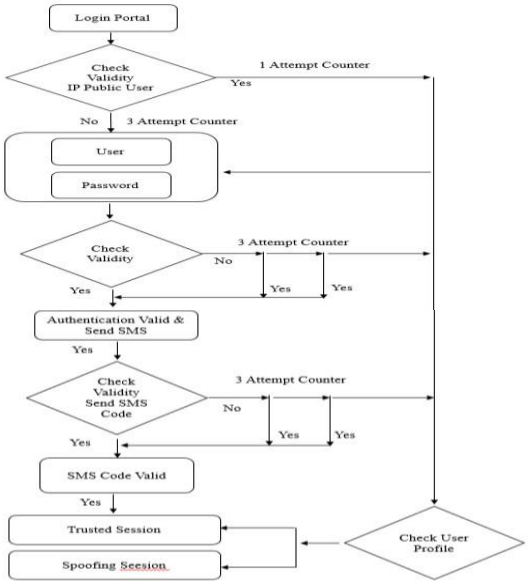

Figure 7: Flows of Login Mechanics

4. Results and Analysis

4.1 Mechanism

At the stage of the security system, trusted users will be registered on the database such as user name, password and phone number are registered. After that the authentication process is developed through three layers that verify the user is trusted if the user and password are entered correctly then automatically included in it do knocking port to mikrotik firewall and followed by entering the verification code sent via short massage to user's phone no user

4.2 Infrastructure Firewall Mechanism

The security system developed can be integrated with system or network infrastructure that has been available, with reference to the concept of security and ease of access. This security system model uses a mikrotik device as a firewall used to close all port access and block all access from the internet. Furthermore, raspberry PI uses Linux operating system which contains webserver and database as storage media detail of trusted user data, public IP information and

as a random code delivery media, from raspberry PI connected with modem shot message gateway as a random message delivery media sent to user via email or short message service. In Figure 8 is a network security infrastructure scheme that can be integrated on the available network, and the three devices are placed in the outermost position on the LAN network as a medium of network security of public access LAN network. This webbased security system with ssl encryption model can be accessed by the user via internet connection using laptop, PC or gadget.

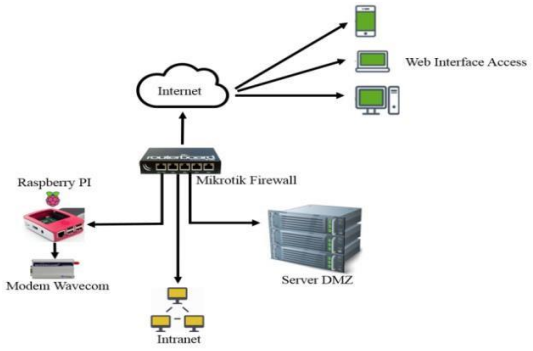

Figure8: Web Knocking Network Infrastructure

4.3 IP Public Verification

Public IP address checks on the database will be performed by the system when the user accesses on the web knocking page, if the IP address used by the user is included in the blacklist, then the user is only given 1 chance to login user, password and short message service code on the web knocking page, otherwise then the user gets 3 times a chance in the input on the web knocking page. The public IP entries in the Blacklist are obtained if a user encounters user login errors, passwords and random code 3 times, the IP address public blacklist will be stored in the database for 60 minutes and after that it will automatically be deleted on the database. Algorithm 1: Public IP

1. Begin
2. Check IP Public
3. If IP Public = Blacklist Then
4. User_Alert> = 1
5. Else
6. If IP_Public = Whitelist Then
7. User_alert> = 3
8. Else

User_Auth_Knock

10. End If
11. End if
12. End

4.4 User Verification

Authentication users are gained by a trusted user after being registered in the database. The user access stage for the information system is done through the web https: //webknocking.xx.xx. After the user is registered by the network admin continued in the stages of the staged security system first stage is when checking the user, password and chaptha entered on the web then the system will verify on the database, if checking the user has made error> = 3 it will receive user information suspend, if not user will get chance 3 times input, if user make error> = 3 then user will disable and will be included in accumulated calculation of suspend user. if not then the system will make the process of knocking through the webserver to the firewall and processproceed to the next stage of receiving random code via email / short message service. In anticipation of error 3 times login time on web knocking page available menu forgot password, before user input user and password if user hesitate or forgot password then user can do password reset by click forgot password by entering email address / telephone number registered in database, if the verification matches then the user will receive a password reset link code via email or the user will receive a random code and input a random code short message service for the creation of a new password.

Figure 9: Web knocking page

Figure 9 is a web knocking portal page https: //webknocking.xx.xx. after checking Public IP used by user and below is process user algorithm auth knock Algoritm 2: User_Auth_Knock

1. User Input, Password, Chapcta
2. Begin
3. Check Dicttionary_Suspend_Count = 0
4. If Check Log_count_Error_login> = 3 Then
5. Suspend
6. Else
7. If User_Auth_Knock> = 3 Then
8. Block_Access
9. Else
10. Activity_Knock1
11. End If
12. End if
13. End

4.5 Knocking Port

Knocking port is a security mechanism that opens a closed firewall port by passing a tap to a firewall with a combination of ports already registered to the firewall. Mikrotik firewall has been integrated with PHP programming language using API.

The step is when the user and password pass the verification in the initial stages, then the web server will do a knock on mikrotik firewall to open a closed port. There are 2 stages of the first tap is the user and password and the second is done opening mikrotik firewall port is when the user passes the short message service code verification. Automatically on the second stage IP public user will be enrolled in whitelist firewall mikrotik to be allowed access to local network source or system information which by default is covered by firewall.

```
[admin@Mikrotik Firewall] /ip firewall filter> print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=input action=accept protocol=tcp src-address-list=LAN dst-port=8291,21,22,23,80,8728 log=no log-prefix=""

 1   chain=input action=add-src-to-address-list protocol=tcp src-address=192.168.0.124 address-list=ketuk1
     address-list-timeout=5m dst-port=9000 log=no log-prefix=""

 2   chain=input action=add-src-to-address-list protocol=tcp src-address=192.168.0.124 src-address-list=ketuk1 address-list=ketuk2
     address-list-timeout=5m dst-port=9100 log=no log-prefix=""

 3   chain=input action=drop protocol=tcp src-address-list=!free dst-port=8291,21,22,23,80,443 log=no log-prefix=""
```

Figure 10: Mikrotik Firewall

In Figure 10 is a mikrotik firewall configuration, line 1 is a combination of first-stage knocking ports to be able to get access knocking permission to the second stage, in the second line is a combination of knocking port to add IP Public user into the address list that can access the local network While on line the third is an access block for access to the local network unless the address list has been entered in the second stage.

Algorithm 3: Activity_Knock1
1. Begin
2. Activity_Knock1
3. If User_Auth_Knock = valid Then
4. Activity_knock1 = http: // ipFirewall: 9000
5. Else
6. Short message service_Code_Knock
7. End If
8. End

4.6 Short Message Service and Email Code

Short message service Code is the final verification stage for opening access of network resources of LAN / information system, system will send short message service code to user which is random code generated in auto generate system. At this stage every user who passes user verification, password and chapcha will receive short message service code and insert on the web nocking page, if the short message service code in the entry does not match the unique code in the database up to 3 times then the user will automatically be blocked and the error will be accumulated at database suspend user, if appropriate then the user system through webserver do knocking to firewall and IP Public user will be given access permission to open firewall port. Automatically a trusted user will log on to the portal page and can access the LAN network.

Figure11: Short Message Service Code Verification

In Figure 10 is the page to enter the verification code obtained by the user via short message service or email.

After successfully entering the short message service code in Figure 12 is the picture when the user has successfully logged on the system security, automatically users will also access system information that is on the network that by default is covered by the firewall.

Figure 12: Portal Login Web knocking

1. Begin
2. Short message service_Code_Knock
3. If Short message service code = valid Then
4. Activity_knock2 = http://ipFirewall:9100
5. Trusted User
6. Else
7. If Alert Count>= 3 Then
8. Block connection
9. Else
10. Suspend
11. End If
12. End If
13. End

For suspended users can contact the network admin to reset the password so that the suspend user count will return to 0, the system if the suspend user status <= 2 will update to 0 if the user has successfully done 3 user login, password and short message service code without errors in different time periods. Here is the information of all user log actives in the database presented in table 1 and table 2, in table 1 it contains about checking public IP status used by user when accessing webknocking page, User status contains about enable, disable, new user Suspend error.

Table 1. User Log Activities

User	IP Public	User Status	Suspend Count	Error Alert Account	Alert Status	Next Alert
antok	Whitelist	Enable	0	1	Allow	Permited
User 1	Blacklist	Disable	6	2	Suspend	Not Permited
Yusuf	Blacklist	Enable	5	3	Suspend	Not Permited
Sumantri	Whitelist	Enable	0	1	Allow	Permited
Anton	Whitelist	Enable	0	1	Allow	Permited
Risky	Whitelist	Disable	2	2	Suspend	Not Permited
Nanang	Blacklist	Disable	3	2	Suspend	Not Permited
Next SMS Code						
antok	Whitelist	New	0	2	Block	Not Permited
Sumantri	Whitelist	Old	0	1	Allow	Trusted User
Anton	Whitelist	Old	0	1	Allow	Trusted User

While in table 2 is the log information of Public IP address of user, access date and user access time successfully access on portal page of knocking.

Table 2 Log Information of Public IP

No	User name	Source IP Address	Alert Date	Alert Time
1	Hariadi	202.xx.xx.xx	03/01/2018	05:10 am
2	User 1	110.xx.xx.xx	03/01/2018	08:15 pm
3	Yusuf	203.xx.xx.xx	20/11/2017	06:03 am
4	Sumantri	158.xx.xx.xx	25/11/2017	11:00 pm
5	Anton	118.xx.xx.xx	01/12/2017	02:15 am
6	Risky	110.xx.xx.xx	05/02/2018	09:10 am
7	Nanang	66.xx.xx.xx	10/05/2018	10:22 pm
8	Romi	118.xx.xx.xx	11/05/2018	08:35 am
9	Bisry	202.xx.xx.xx	22/06/2018	09:25 pm
10	Fuad	110.xx.xx.xx	18/06/2018	10:10 pm

4.7 Penetration Testing Webknocking

In this study the tests were conducted to test the vulnerability or vulnerability of the web or known as the penetration test (pentest) on webknocking pages. In pentest tools used is to use nmap port scanner to view the open port and use nikto tools to do web knocking vulnerability testing.

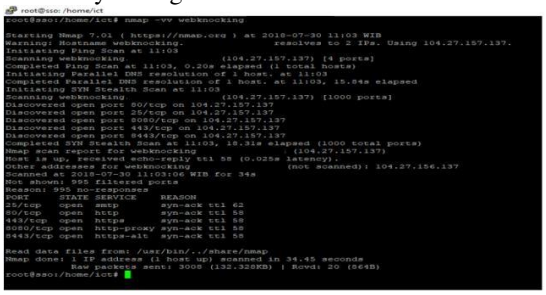

Figure 13 Port Scanning

Based on Figure 13, the port scaning results show an open port of 80 for web, 443 for https, 25 for smtp and 8443 for http-alt. Public IP used webknocking has been secured using proxy in cloudflare. From the analysis of the webknocking does not open the port used to perform the opening knock of the firewall on ports 9100 and 9200. So not visible when the scaning port from the internet.

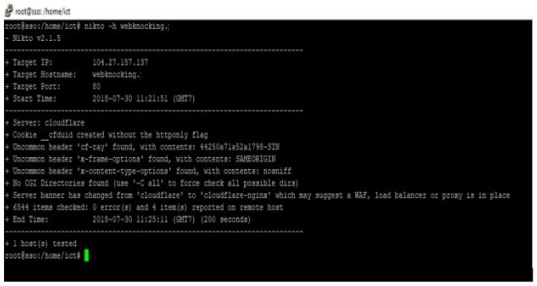

Figure 14 Vulnerability test

Based on Figure 14, the results of the analysis of vulnerability checking from web webknocking, from the web application nikto webserver web application aplication firewall (WAF) from cloudflare, so that if not found a dangerous vulnerability.

5. Conclusion and Suggestion

Security issues will be a challenge for any industry, sometimes for mature industries with adequate resources often facing security issues. The purpose of this research is to develop and implement security intelligence for the industry with user-friendly system and can be integrated with existing network with relatively cheaper cost. So for some middle

and lower industry that the difficulties in the implementation of security in information systems can implement this security system with easy use.

This security system has been tested using security penetration test tools with results that have been as expected that no ports are open and little vulnerability is found. Perhaps in its development penetration test can use other tools

6. Future Scopes

The system can further be enhanced by providing various options. Adding advance intelligence security will be more given secure operating activities to organization. The development of intelligence security in services industries i.e. banking sector and hospitals were next opportunity to build and develop security information system. More effective and robust security intelligence becomes the next research challenge in the future

References

[1] Yampolskiy R. V. 2014, Utility Function Security in Artificially Intelegent Agent. *Journal of Experimental & Theoretical Artificial Intelligence*. Sep2014, Vol. 26 Issue 3, p373-389. 17p. DOI: 10.1080/0952813X.2014.895114

[2] Ratna S. R., Ravi, R., &Shekhar, B., 2015, An Intelligent Approach Based on Neuro Fuzzy Detachment Scheme for Preventing, Jamming Attack in Wireless Networks. Journal of Intelligent & Fuzzy Systems. 2015, Vol. 28 Issue 2, p809-820. 12p. DOI: 10.3233/IFS-141363

[3] Bouzar B. L., Bouabana, T. T., &Benferhat, S., 2015, Instantiated first order Qualitative Choice Logic for an efficient handling of alerts correlation. Intelligent Data Analysis. 2015, Vol. 19 Issue 1, p3-27. 25p. DOI: 10.3233/IDA-140693

[4] Blazek P., Kuca, K., Jun, D., &Krejcar, O., 2017, Development of Information and management System for laboratory based on Open Source Licensed Software With Security Logs Extension. Journal of Intelligent & Fuzzy Systems. 2017, Vol. 32 Issue 2, p1497-1508. 12p. DOI: 10.3233/JIFS-169145

[5] Sobeslav V., Balik, L., Hornig, O., Horalek, Josef.,&Krejcar, O., 2017, Endpoint Firewall for Local Hardening in Academic esearch Environment. 2017. Journal of Intelligent & Fuzzy Systems, Vol. 32 Issue 2, p1475-1484. 10p. DOI: 10.3233/JIFS-169143

[6] Computer Network

[7] Stallings W., & Brown, L., Computer Security Principles and Practice, Second. 2012

[8] Anderson C., Baskerville, R. L., Kaul, M., 2017, Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. Journal of Management Information Systems. 2017, Vol. 34 Issue 4, p1082-1112. 31p. 4 Diagrams, 2 Charts, 1 Graph. DOI: 10.1080/07421222.2017.1394063

[9] De Souza, C.S.P., da Silva, S., & Jose, A., 2017, Security Management Benefit at Work in Monitoring Individual Protection Equipment (IPE) and Collective Security Systems (CSS), Procedures and Methodes in Industry Construction. Business Management Dynamics. Jan2017, Vol. 6 Issue 7, p19-26. 8p

[10] Sobeslav V., Balik, L., Hornig, O., Horalek, J., &Krejcar, O., 2017. Endpoint Firewall for Local Security Hardening in Academic Research Environment . Journal of Intelligent & Fuzzy Systems. 2017, Vol. 32 Issue 2, p1475-1484. 10p. DOI: 10.3233/JIFS-1691

[11] N. Yrvina. 2017. Cyber security Tips to Keep Your Firm Safe. Journal of Financial Planning. Jan2017, Vol. 30

[12] Herranz J., & Nin, J., 2014, Secure and Efficient AnonymizationOf Distributed Confidential Databases. International Journal of Information Security. Nov2014, Vol. 13 Issue 6, p497-512. 16p. DOI: 10.1007/s10207-014-0237-x

[13] Vavilis S., &Petkovic, M., Zannone, N., 2016, A Severity –Based Quantification Of Data Leakages in Database Systems. Journal of Computer Security. 2016, Vol. 24 Issue 3, p321-345. 25p. DOI: 10.3233/JCS-160543

[14] Hadavi M., Jalili, Rasool.,Damiani, E., &Cimato, S., 2015, Security and Searchability in Scret Sharing-Based Data Outsourcing. International Journal of Information Security. Nov2015, Vol. 14 Issue 6, p513-529. 17p. DOI: 10.1007/s 10207-015- 0277-x

[15] Chaniotis I., Kyriakou, K.I., & Tselikas, N., 2015, is Node. Js aVisible Option for Building Modern Web Applications? A Performance Evaluation Study. Computing. Oct2015, Vol. 97 Issue 10, p1023-1044. 22p. DOI: 10.1007/s00607-014-0394-9