Heimdallr[1]: A system design for the next generation of IoTs

Ayberk Aksoy Bipin C. Desai
CSE, Concordia University, Montreal Canada
{a_aksoy@encs.concordia.ca, BipinC.Desai@concordia.ca}

Abstract

In today's wired and interconnected world, a sheer number of devices are now able to be connected to the internet and expose the data generated by user inputs or the devices' built-in sensors. These growing numbers of internet of things (IoT) devices are called smart and they range from mobile phones, smart televisions, IP cameras, household and industrial appliances, to Wi-Fi thermostats and thermometers. The reason for the avalanche of IoT devices is their convenience and remote accessibility over the traditional versions. However, as with other technological breakthroughs, IoT have a major issue regarding the security of access and control of the data generated and hence privacy.

To address these issues, we propose in this paper a system based approach: the system consists of two parts to monitor users' IoTs. The first aspect of this system is a firewall monitoring and controlling the incoming and outgoing traffic to and from the IoT devices which are connected to the internet via a new generation of routers called Heimdallr. The second aspect is to store locally in this router the user's IoT related data and allow a secure interaction by the user with the data and the IoTs. A third concept introduced in the system to ensure that any updates to the IoT software is verified and certified by a central not-for-profit organization. Heimdallr would not allow any updates to the software to be made unless the update has been certified by this certification agency. The certification agency has a role similar to CSA [1] or UL [2] organizations which provide testing, inspection and certification service and are involved in setting standards. It is worth pointing out that currently in the software domain, all this is done by the for profit corporation without any public oversight. The only beacon is the open source community where

[1] Heimdallr, in the Norse mythology, is the gods' watchman having acute hearing and eyesight.

dedicated developers donate their time, talent and energy to produce open source software which is often free and the source code is accessible to anyone to investigate and verify their algorithms and functions.

1 Introduction

Like many of today's smart devices, an internet of things (IoT) claims to be smart. These smart devices replace the function of some traditional device with the ability of not only replacing the function, perhaps using other technology, but adding a feature to have a wireless connection (Wi-Fi). This Wi-Fi feature is needed to connect the device to some transmission device, usually a cell phone (another smart device). In the cell phone an ad hoc software program (an app) is used to complete the connection of the device to a server which is usually operated and controlled by the manufacturer of the IoT device. This connection is used to transmit data from and to the IoT device and provide remote access. The smarts in these devices replace the mental or temporary recording of the status of some data: the app and its infrastructure takes over this operation adding some convenience to 'justify' the higher cost and effort of replacing the old and tried traditional device.

Many issues with IoT devices and networks are being noticed today: this reminds one of the days of wild west when entire indigenous communities were wiped out by the advancing hordes of immigrant settlers with guns and artillery. Personal privacy is perhaps the most important victim of this digital age wild west massacre. The first weakness in IoTs is that their software developed is usually rushed by the organization introducing these devices with apparent lack of thought about security and privacy. The second issue is the lack of safeguard of the user data which is made available, for profit, to third parties. Hence the data subjects (original generators of the data) lose control of their data which exposes them to uninvited marketing and manipulation. All small incremental data, when aggregated by various players of this digital age gives what we call big data. Big data and the governmental *laissez-faire* attitude has lead the exploitation of this data and has given rise to mammoth new so called tech companies. One of the most obvious and profitable way of exploiting user data, collected and aggregated from users, is to enable the marketing of targeted ads. For instance, the annual advertising revenue of one of these tech giants, for the 2018, exceeded 110 billion US dollars forming the major percent of this company's total

revenues in that year of over 130 billion US dollars [3], [4]. Decades of research in marketing has concluded that rather than global publicity, targeted ads are what make the difference. In order to gain such data leverage the company keeps track of all the users of their 'free' services– along with their actions, sites visited, text communications and choices, analyzes them against past usage and create profiles which guide their software to choose the most pertinent tailored targeted ads. However, they don't stop there and this is exactly where the problem arises.

In order to increase profit, these companies with big data sell user profiles to other companies who in turn can do the same. For instance Facebook, allow personal data to be used by paying third parties as Mark Zuckerberg revealed during his testimony before the Congress on April 10, 2018. During the testimony it was revealed that Aleksandr Kogan, a onetime lecturer at Cambridge University, had developed a survey application on Facebook platform and using the access given by Facebook, was able to assemble the data of all friends of any user who took the survey. Access to the friends data, without the consent of these friends, was a feature of Facebook and any of the thousands of applications developed for the platform had access to the users' and their friends data [5], [6].

Similar story is heard about other big tech companies as well. Google collects its users' data and sells them to other companies without data owners' awareness. As Douglas MacMillan stated in one of his articles in the Wall Street Journal (WSJ), Google let hundreds of outside developers use the data scanned from the in-box of users who have signed up for 'free' email-based services [7]. Furthermore, according to Google allow these outside developers to share what they collect with other third parties. In a letter from Susan Molinari, former vice president for public policy at Google, "Developers may share data with third parties so long as they are transparent with the users about how they are using the data," she wrote, according to a WSJ article on September 20, 2018 [8]. It is not clear what this transparency means and or allows.

Among all other big companies with billions of users' personal data, Amazon stands out the most when it comes to selling targeted ads, even though, it has only around ten percent of Google or Facebook's big data. Since advertisers value the most accurate information they can get on what people actually buy and what they are likely to buy soon, this can be gleaned from the Amazon marketing platform. Knowing that, the contents of according to another report from WSJ, even

their employees leak data for cash rewards [9]. It appears that these big tech mammoths are not living up to their own privacy policy which they can change without any oversight.

These reports were only some incidents related to services that users access using an internet browser. Now one may start to wonder, how much data we are giving away by just buying IoT devices and bringing them into our homes. Amazon Echo and Google Home are such examples. Every word that the users say may not be sent to the cloud by those devices, but they are always listening to be able to recognize their wake word and this can lead to some serious privacy breaches. Furthermore, Amazon Echo and Google Home are legitimate devices made by world giants who have so to speak strict privacy policies. But what about the other IoT devices, some are start-ups, which are rushed to be made available for profit and lacks safeguards regarding user privacy and data security? Do these companies which have access to user profiles have any policies or ethical code and how are they regulated?

Another example of IoT replacing traditional devices is a smart body thermometer. The traditional mercury in a glass tube clinical thermometer, was invented in 1724 by Daniel Gabriel Fahrenheit. It has been used since [10]. It needs no battery and is ready for use even after years of non-use; the only tricky part is to shake down the mercury to reset it. This classical clinical thermometer has been replaced by a digital version which requires a battery needing regular replacement. Both these are now being displaced by a smart body temperature thermometer by Kinsa Company which is a case in point. These internet-connected thermometers, replacing the traditional mercury column in glass versions and even the ordinary digital ones, are now in more than 500,000 households [11]. These thermometers send the data to an application in a cellphone to track the temperature; however, the data is also sent to the device manufacturing company. During the flu season of 2018 the Clorox Company paid to license information from Kinsa, according to NYT [12]. Kinsa also sells this data to other companies under the name of Kinsa Insights to be used to target advertising [12].

This is only one such example of how the users lose control over their personal data and privacy. Perhaps, losing control over the private data which consists of the user's first name, family name and email address might not be an issue to some extent, however, if this data gives away information about user's daily routine, this can lead to some serious unwanted consequences. Smart thermostats which allow users to see and alter the current temperature of their houses

remotely, carries such data. As an example, if a smart thermostat company provides this user data to paying third parties, a misuse of that data could reveal the absence of the house owner at low temperatures. Those kind of contemporary issues in the IoT sector show the importance of privacy, security and the user having control over their own data.

2 Proposed System

Along with the contemporary problems that exist in current in IoT network, there would be other serious issues with their proliferation and usage in people's private lives e.g., IP cameras, baby monitors, smart menstrual period trackers etc. An article from BBC says "Although the baby tech sector specifically is relatively young and unstudied, researchers from market research firm Hexa say the baby-monitoring sub-market alone is projected to grow from $929m in 2016 to $1.63bn by 2025" [13]. Therefore, with this dramatic increase, more users will be losing control over their data and the increasing loss of privacy would lead to worse consequences.

To address this problem of such data piracy, we propose, in this paper, a system called Heimdallr that builds a fortress around users' private networks to protect the data generated and used by IoT devices and lets the users take control over it.

Heimdallr is a software that would run on user's next generation personal wireless smart router: itself an IoT! The main idea behind the Heimdallr system is to allow users full control over their data by first, monitoring and manipulating the network traffic on the router and secondly, running all the necessary services locally (in the router) for users to have access to full features of their connected IoT devices without the need of a connection to any server of any of the IoT makers. To realize such a complex task, IoT device makers would be required to develop Heimdallr compatible user interfaces and services along with their IoT products. Since Heimdallr is the gate keeper, all interaction with any IoT is under its guard, including those coming from mobile phones! This obliges us to state the underlying requirements for the system.

2.1 Requirements

The proposed solution has to have three main requirements to be fully functional. The most essential one is a central non-profit software certification organization; we have named the

Software Assurance Agency or SAA. It is introduced to be responsible for testing, inspecting, storing and certifying software from device interfaces and updates to the services provided by IoT device makers. The concept intends to prevent two things. Prohibition of software which lacks required privacy measures which could threaten users' private data and monitoring of software updates that could alter IoT operations and introduce unwanted features without users' consent. Thus, SAA will guarantee that all software, certified by this organization, does exactly what it is supposed to and does not poses any threat to user's privacy. Put simply, SAA introduces some measure of standardization for IoT devices as has been done by organizations such as UL [2] and CSA [1]. We envisage that SAA would remain independent and not become a front for IoT industry as has been the case with some of the recent organizations which are directly or indirectly the essentially public relations surrogate for the industry [14], [15].

The second requirement is to have static IP assigned to our 'smart' routers equipped with higher-end hardware over the routers we use today and including a computing system[2]. This is required, since, Heimdallr is intended to be run on user's router being the gateway for IoT devices to the Internet, and therefore, it must have the minimum system requirements to be able to run the Heimdallr software and the required services of the IoT devices as discussed in this paper.

The final issue that this system has to deal with is the need to be accepted by the tech companies worldwide. Under the current circumstances, most of the companies, especially the tech giants, would not want the supervision of Heimdallr, given the profit that they are reaping from users' private data. Regarding that, imposing either administrative or social sanctions or both can be considered as a possible solution as long as there exist users who are concerned about the privacy of their data. In any case, such concerns would create legal, societal and competitive pressure for an IoT device maker to support and use the certification authority, SAA.

---

[2] We envisage Heimdallr to be equipped with an economic computing devices such as Raspberry Pi and storage. What we are aiming for is the pendulum to swing back and bring back home the user data from the cloud!

2.2 Problems Addressed

In this section, different types of problems that the Heimdallr system addresses are explained in detail.

2.2.1 Supply Company related issues

As discussed in the introduction, recent experience with manipulating user data for political gain amply illustrates that unregulated tech companies are not necessarily the organizations that should be trusted with user data privacy and security [16], [17]. Although not every company is selling user data for profit, non-the-less many of them still have other problems. Third-party services are one of the most common examples of this issue. Many small and big IoT companies use third-party services in their products to provide additional features to users without their consent. A study on IoT devices shows along with many other examples that "During the first minute after power-on, the Samsung Smart TV talks to Google Play, Double Click, Netflix, FandangoNOW, Spotify, CBS, MSNBC, NFL, Deezer, and Facebook—even though we did not sign in or create accounts with any of them" [18]. The same study says, "The Geeni smart bulb communicates with gw.tuyaus.com, which is operated by TuYa, a China-based company and also offers an MQTT service, which allows the manufacturer to communicate with their device in a user's home; apparently done without the knowledge or permission of the user" [18]. Therefore, not only users have lost the control over their data, there is no guarantee that these third-party services will not do anything harmful with it. For all these reasons, Heimdallr system requires all IoT device makers to develop Heimdallr compatible user interface and services that will run locally. This would produce two desirable results. First, none of the IoT devices will be required to use any known or unknown services on the Internet, which means that user data will flow only between the user and the IoT device via Heimdallr and go nowhere else,; second, all data that the IoT devices consume can be monitored, changed, collected and deleted by the user with the intermediary Heimdallr. As a conclusion, there will be no reason to have unwanted data leaks since users have the full control over their data.

Another problem with keeping hundreds of thousands of user profiles in company databases is that it basically creates a bigger risk of data theft. People do not just use one service or a single IoT device, but they use products of dozens of different companies. Even with a single product, a user's data gets stored in the device maker's database, as well as databases of all third-party services that

this product works with. Therefore, in a real life case where a single user owns several products, duplication and storage of their private data in a number of locations increases gradually. This raises the threat to data privacy, since, the same user's data is stored in an unknown number of different databases with different security measures and vulnerabilities. While, one company might be able protect users' data in a difficult situation, another one could fail to do so under the exact same circumstances. Similarly, an article posted on Electronic Privacy Information Center's website says, "In another sense, control can be lost as more and more companies collect data about users. This data often paints a detailed picture of individual users through the collection of activities online" [19]. This indicates that keeping the personal data securely, in one place is definitely a step that must be taken on the way to secure it. With Heimdallr user data will only be stored locally in Heimdallr's database. Thus, one can be sure that the data is secure as long as the Heimdallr is. Additionally, since every user will have an independent Heimdallr system, there will be less private data stored in any database. Therefore, as Apple CEO Tim Cook says, "No one should have a key that turns a billion locks. It shouldn't exist. No one should have the message content for all of these messages. You wouldn't want it all in one place. I think it would be very bad for security and privacy" [20] in an interview with TIME's Nancy Gibbs, when the effort needed to penetrate billions of Heimdallr systems is compared to its reward, it becomes less attractive for intruders who are seeking to violate others privacy.

2.2.2 Hardware/Software related issues

IoT related problems do not always stem from companies' privacy policies. They sometimes arise from rushed or imperfect software development which lacks essential security measures. Non-technical or even the technical users may not be able to notice a defect in a software which leads to serious violation of data privacy. Given the fact that those programs are embedded and working in IoT devices, it becomes nearly impossible for any user to analyze them. Additionally, "Most IoT devices do not mention the specific third parties they communicate with in their privacy policies, which makes it difficult for consumers to make purchasing decisions based on security and privacy considerations" says the study mentioned earlier [18]. Introduction of SAA plays an essential role here. Trustfulness of the software used in IoT devices is guaranteed for maximum safety of personal data and privacy by a not-for-profit open organization.

Every IoT device consists of both software and hardware, and therefore, both aspects have to be considered for probable vulnerabilities. An article from Malmö University that supports this idea says, “Appliance manufacturers don’t always think like established software developers do in terms of, for instance, security and quality criteria in the development phase. Quite the contrary, actually. And the embedded systems in the Internet of things, are often developed by using existing chips and designs, and the quality or security criteria in their development process there are unknown” [21]. For that matter, while SAA is offering a solution to software defects, Heimdallr will be protecting the integrity of user data against any kind of hardware exploits to prevent unwanted breaches. Heimdallr achieves this by monitoring and controlling the incoming and outgoing data traffic to and from the IoT devices in the network. It will allow only the requests from IP addresses which are either whitelisted or not blacklisted with valid cookies, while blocking all the other data flow to and from any device. Heimdallr also provides its users secure access to IoT devices connected to it by building a firewall which checks user credentials and user’s current location. Thus, even if there are any hardware issues that pose a risk to user privacy, without the permission of the actual user, the integrity of private data will be ensured.

Enforcing generalized security measures can be pretty difficult when it comes to IoTs. One of the techniques used is to create a generalized protection mechanism and if it works on the test system, it is assumed to work on all similar systems. It is assumed that his principal would work for IoTs; however, since IoTs borrow heavily from existing technologies and have to be used in differing environments the adaption is not straight forward. Thought about security and privacy are not paramount in the design and implementation of the core components, of both hardware and software of IoTs [21]. Instead of per device protection, Heimdallr offers a generalized solution by creating a safe zone for all IoT devices in its network as it is mentioned above.

A final software related issue worth mentioning is the complex nature of the security procedures involved in the server connections established between the user, IoT device and the server that provides the necessary services. Instead of depending on unknown procedures, and protocol for security and privacy of each type of IoTs, it is preferable to come up with an open standard and its implementation to avoid denial of service or privacy breaches [22]. Thus, Heimdallr provides the necessary protocols and services to its established users securely. That means, instead of thousands of clients trying to access the same service on a server for a given IoT device, only a limited

number of authenticated users would have regular access to the IoTs. Direction of the authenticated users' request into their dedicated Heimdallr system by-passes the IoT makers' server. The only load on the server would be requests to the SAA for registering updates to firmware and creating certificate for these updates. Heimdallr would make periodic requests for updates to the SAA.

This solution that Heimdallr provides solves another serious contemporary issue with IoT devices, namely Distributed Denial of Service (DDoS) attacks. In August 2016, a botnet called Mirai was first identified by the whitehat security group MalwareMustDie. Right after, in September 2016, according to Kolias et al [23]. Website of Brian Krebs, a computer security consultant, was hit with 620 Gbps of traffic. The principle behind Mirai botnet is to first scan random public IP addresses through the telnet protocol (TCP port 23 or 2323) and try to log in to any IoT device discovered using just 62 possible default username-password pairs. Once the access is gained, Mirai gets control of that device to be used for further DDoS attacks. However, Heimdallr natively prevents this thanks to its firewall. In order for a request to reach an IoT device in the Heimdallr network, the requester has to first successfully enter the user-defined credentials, and secondly, the origin of the request must be white listed by the user. If a malware like Mirai botnet try to intrude on an IoT device connected to Heimdallr, it would cut the connection immediately with that origin and blacklist it. Furthermore, if an IoT device gets infected by such a malware, a DDoS attack cannot be launched with that device, since, Heimdallr would not allow any data to pass through unless the target IP is whitelisted or the HTTPS packet that is sent carries a valid cookie.

3 Architecture of Heimdallr

Implementation of the Heimdallr system, while intuitively simple, requires complex acceptance issues which are beyond the realm of a technical paper. Aside from its exigent requirements for this idea to work, the intended features for Heimdallr needs a team of dedicated developers, funds, and most importantly time. However, to validate our concept, we have implemented a dry-run-test version of the proposed system to be tested and evaluated to see its competency. In this section, we provide high level design of the Heimdallr system which was used for our proof of concept.

3.1 System Diagrams

In order to see how the final product may look and function, we implemented the essential components of a real life scenario of an IoT device usage supported by the Heimdallr system. Note that the diagrams shown below represent not the actual implementation of the proposed solution but a proof-of-concept version of the devices which have a role in such a scenario. This includes the implementation of a *Client Device,* an *IoT Device, Heimdallr, IoT Device Maker,* and *SAA.* Figure 1 gives the Deployment diagram of the proposed system; Figure 2 gives a Use Case and Figure 3 depicts the Sequence diagrams of our proof-of-concept system.

3.1.1 Deployment Diagram

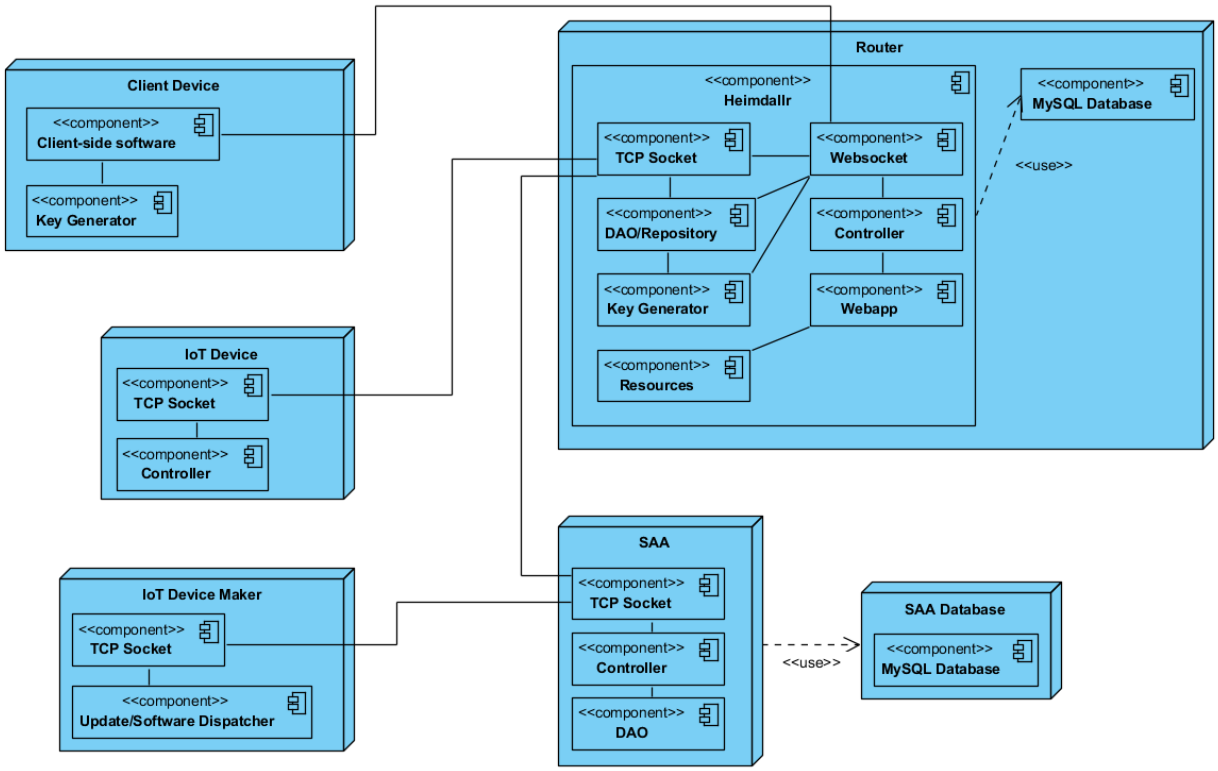

Figure 1**: Deployment Diagram of the proposed system**
This figure shows the relationship between hardware and software components of the complete system

In the Deployment diagram above, the overall system design and the relationship between all the involved hardware and software components are indicated. The system is composed of mainly five hardware components plus a database for SAA. Those are *Client Device, IoT Device, IoT Device*

Maker, user home smart *Router*, and finally *SAA*. A client device is what enables users' to connect to their Heimdallr installed router. It hosts the key generator software that generates access codes for first time logins on new devices and another client-side software such as a web browser or an application with a UI to interact with their Heimdallr. An IoT device is an internet connected device like a smart thermostat which is to be controlled by the client device in our tests via Heimdallr. It consists of a single program which allows the device to connect to Heimdallr through its TCP socket and processes every task –in its controller– sent by the client device to Heimdallr and then redirected to it.

IoT device makers, instead of accessing their IoTs directly would simply change their procedures; the change requires them to register their product with the SAA and upload all initialization and update codes to the SAA along with all necessary documentation changes implemented and the reason for the changes. The documentation must be public and open and accessible from the device maker or SAA. SAA is the main source for all software and their certification; all software for all SAA registered IoTs is accessible from it.

Once any software from IoT device maker initiates a certification process with the SAA and if the certification process is successful, the software is ready for distribution; if not the IoT maker is notified and the software is in a hold status until a satisfactory update is made for, and a new request for certification. A certified software is passed on to the Data Access Object (DAO – the software repository) of the SAA and required details are stored in the SAA's database. SAA is also connected to Heimdallr through its TCP socket and responsible for delivering the requested software (product) or update to Heimdallr when needed.

The final component shown in Figure 1 is the Heimdallr router. Here the router is the high-end hardware running the Heimdallr software and a database connected to that. There are seven main components that we can classify in Heimdallr. *TCP Socket, Websocket, DAO/Repository, Controller, Key Generator, Webapp,* and *Resources.* TCP socket allows it to connect to the other elements, particularly to the IoT device and SAA. Web socket along with web app component provide a real-time UI –stored in resources– to the client device. DAO (repository) is responsible for database related operations such as checking the user credentials or adding a new IP address to the white-list. Controller is the heart of the Heimdallr where every request made to it is processed.

It redirects users to correct pages, manages all the security related tasks, and passes all required information to and from the client device and the IoT device.

3.1.2 Use Case Diagram

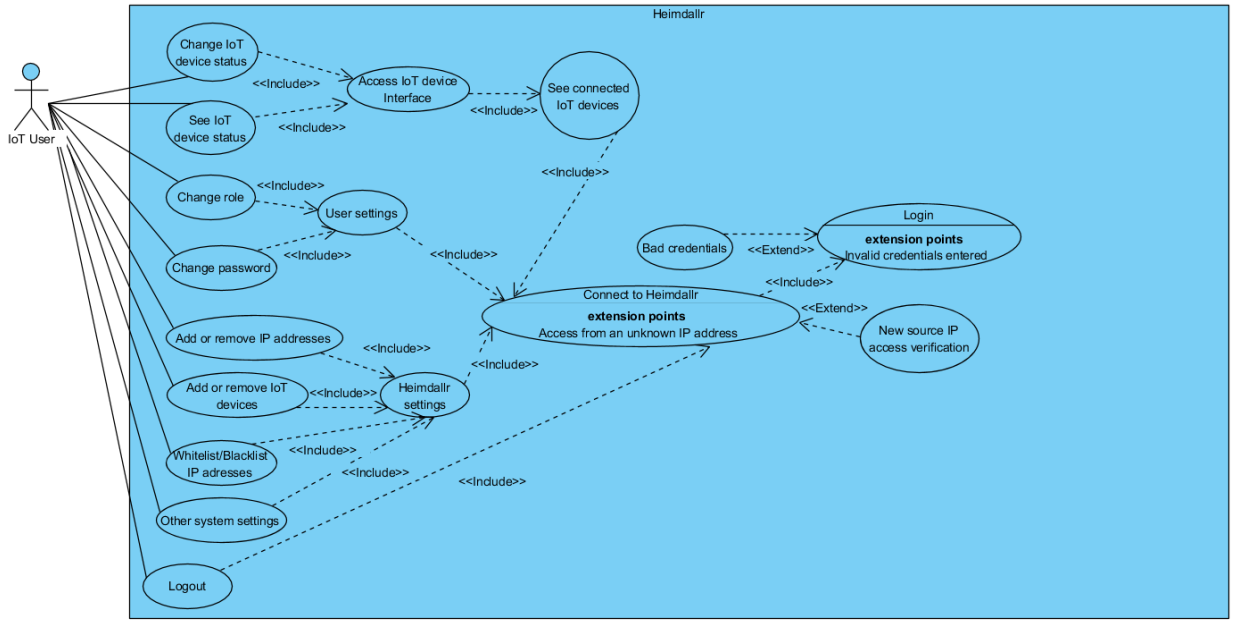

Figure 2**: Heimdallr Use Case Diagram**
This figure shows the interaction of an IoT user with the Heimdallr system

In the Use Case diagram above the interaction of a user with Heimdallr and the possible actions are shown. A user can control an IoT device by means of seeing and altering its current status. User also can see all of the owned connected IoT devices, change currently assigned role (user or admin), change username and password, add or remove IP addresses and whitelist or blacklist them, sign out from a client device (e.g. a web browser) by invalidating its cookie, connect new or remove registered IoT devices, login and finally logout. In the diagram above, it is shown that every action requires the user to first connect to the Heimdallr and then login before taking any other actions. Login action can lead to another action called bad credentials where the user is prompted to re-enter the correct username-password pair or an access code generated with the key generator.

3.1.3 Sequence Diagram

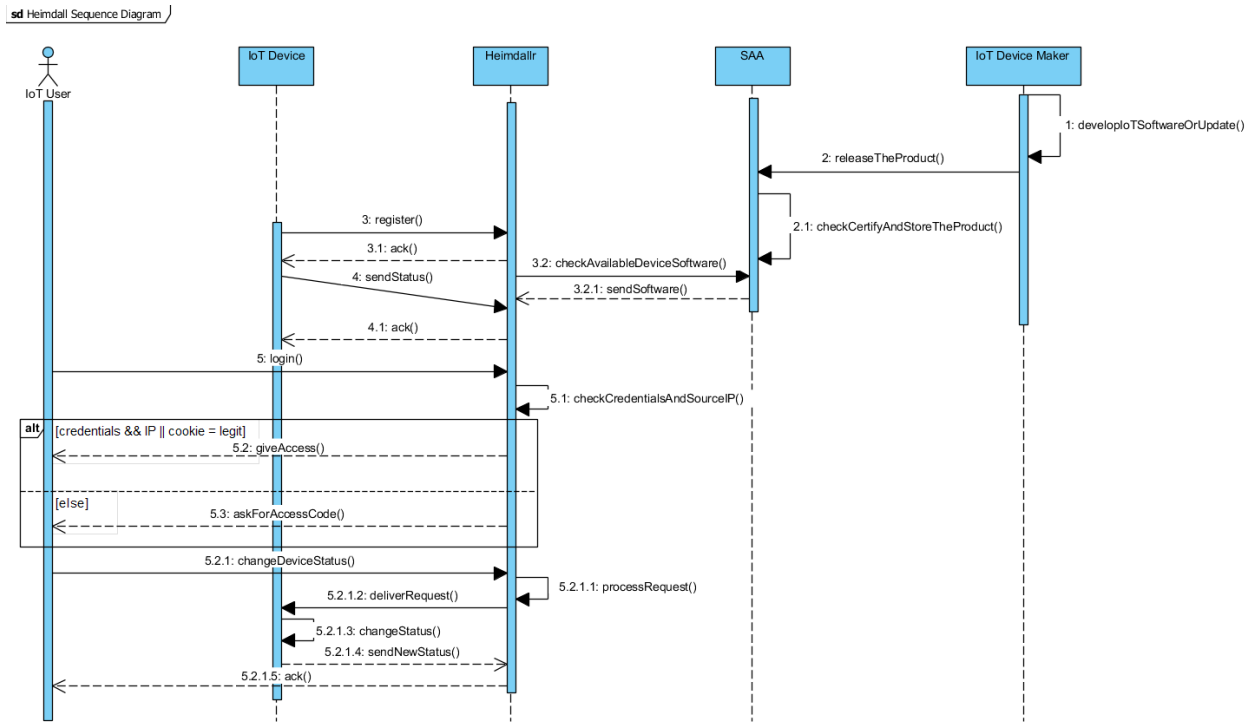

Figure 3**: Sequence Diagram of the proposed solution**
This figure shows the interactions of the components (elements) sequentially for a given time period

In the Sequence diagram given in Figure 3 the interactions of the actors (elements) of the system are shown in a timeline. From left to right the actors are aligned and the period of time starts at the top and ends at the bottom. Thus, the very first action is taken by the *IoT Device Maker* by developing and releasing the product for an IoT device. Then, *SAA* receives and checks it and if it decides that the product has no security flaws, certifies and stores it. Meanwhile, an *IoT Device* requests registration to *Heimdallr* and *Heimdallr* checks if any service or update is available to download for that device in *SAA* database. Right after the registration of the *IoT Device* is completed an *IoT User* requests login to *Heimdallr*. If user credentials are correct, the cookie sent in the https packet is valid and the IP address of the requester is not blacklisted *Heimdallr* grants the access. After that, user can take any action given in Figure 2.

3.2 Preliminary Experimentations

With a working proof-of-concept simulator of Heimdallr system, we first checked the integrity of the system to make sure that there were no flaws within the basic functionality. Every use case is tested with a single user and single IoT device, single user and multiple IoT devices, multiple users and single IoT device, and multiple users and multiple IoT devices using different IP addresses. Since one part of the Heimdallr is a web application, the system must be robust enough to be able to negate every kind of known web attack for absolute security. For now, during our tests only the most common attacks on web services are simulated namely Cross-site Scripting (XSS), SQL Injection, and Cross-site Request Forgery. We plan to do further experimentation for other types of potential vulnerabilities. Hence in the next part in the development work, all known attacks will be tested and any vulnerabilities found would be addressed. We also make sure that Hypertext Transfer Protocol Secure (HTTPS) is the only protocol to communicate with Heimdallr to increase security. Finally, we tested the consistency of our Key Generator algorithm to make sure that two-factor authentication works flawlessly when a request is made from a new IP address and doesn't carry a valid cookie.

During our tests, we noticed that an essential feature was posing a security risk. We were using MAC addresses when registering an IoT device to Heimdallr. However, an attacker can eavesdrop on the packets that is sent from a wirelessly connected IoT device and through MAC spoofing, an unknown IoT device can impersonate that registered device and gain access to Heimdallr. Since, one has to physically access a device to get its serial number, we decided to use it and the device's name when registering to prevent MAC spoofing and related attacks.

Overall the current version of the Heimdallr system works as intended with all the basic functionality after all of the tests on which we ran in local network. However, even though the idea of this system showed its competency to deal with the current IoT related issues in our tests, we concluded that for more accurate results, an alpha prototype should be implemented and tested in a typical real usage replication with a mix of simulated smart IoTs.

4 Conclusions and Future Work

IoT devices are proliferating and becoming every day tools for the ordinary person. The ubiquity of these devices allows us to see them even in the private moments of our lives. The access of the data that we provide to IoT device makers –by using these devices, exposes our habits, routine and schedule in addition to the base data given up in good faith. Thus, all the security issues related to data exposed to the IoT device suppliers and the third parties they use and the vulnerabilities hidden in the IoT devices' hardware and software is becoming a more serious threat to privacy. As a result of our study of those issues we realize that as long as an IoT device is able to access the internet freely, privacy of the user data is compromised. For this reason we created the Heimdallr system. Heimdallr can be described as a guardian that enhances the function of the users' home routers. It monitors and controls the incoming and outgoing data traffic to and from the IoT devices connected to it and only allows requests from authorized users from whitelisted IP addresses and/or having secure credentials including a valid cookie. Additionally, it is able to connect to SAA for access to all certified software and its updates for an IoT device. The system thus guarantees that the users' private data flows only between the IoT device and the user.

Our plan is the implementation of an alpha version of this system. Since all data passes through the Heimdallr, it can collect all data and updates for later reference while having all of it under the control and possession of the owner of the system [24].

We see our system as the start of the swing of the pendulum to the era were the data subject did not need outside for-profit data storage service(cloud) and would lead to other development to re-create privacy preserving version of what is being offered by today's big tech companies. With judicial user interface, operation of Heimdallr would be made as easy as some of the better mobile phones; suitable for the tech non-savvy!

References

[1] C. Group, CSA Group, [Online]. Available: https://www.csagroup.org/. [Accessed 6 March 2019].

[2] U. LLC, "About UL," UL LLC, [Online]. Available: https://www.ul.com/aboutul/. [Accessed 6 March 2019].

[3] Satista, "Advertising revenue of Google from 2001 to 2018 (in billion U.S. dollars)," Satista, February 2019. [Online]. Available: https://www.statista.com/statistics/266249/advertising-revenue-of-google/. [Accessed 5 March 2019].

[4] Satista, "Annual revenue of Google from 2002 to 2018 (in billion U.S. dollars)," Satista, February 2019. [Online]. Available: https://www.statista.com/statistics/266206/googles-annual-global-revenue/. [Accessed 5 March 2019].

[5] L. Stahl, "Aleksandr Kogan: The link between Cambridge Analytica and Facebook," CBS News, 22 April 2018. [Online]. Available: https://www.cbsnews.com/news/aleksandr-kogan-the-link-between-cambridge-analytica-and-facebook/. [Accessed 7 March 2019].

[6] J. C. Wong, "Mark Zuckerberg faces tough questions in two-day congressional testimony – as it happened," The Guardian, 11 April 2018. [Online]. Available: https://www.theguardian.com/technology/live/2018/apr/11/mark-zuckerberg-testimony-live-updates-house-congress-cambridge-analytica?page=with:block-5ace2921e4b08f6cf5be55e4#block-5ace2921e4b08f6cf5be55e4. [Accessed 4 March 2019].

[7] D. MacMillan, "Tech's 'Dirty Secret': The App Developers Sifting Through Your Gmail," The Wall Street Journal, 2 July 2018. [Online]. Available: https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442. [Accessed 5 March 2019].

[8] J. D. McKinnon and D. MacMillan, "Google Says It Continues to Allow Apps to Scan Data From Gmail Accounts," The Wall Street Journal, 20 September 2018. [Online]. Available: https://www.wsj.com/articles/google-says-it-continues-to-allow-apps-to-scan-data-from-gmail-accounts-1537459989. [Accessed 5 March 2019].

[9] J. Emont, L. Stevens and R. MacMillan, "Amazon Investigates Employees Leaking Data for Bribes," The Wall Street Journal, 16 September 2018. [Online]. Available: https://www.wsj.com/articles/amazon-investigates-employees-leaking-data-for-bribes-1537106401. [Accessed 5 March 2019].

[10] M. Bellis, "The History of the Thermometer," ThoughtCo, 27 November 2018. [Online]. Available: https://www.thoughtco.com/the-history-of-the-thermometer-1992525. [Accessed 6 March 2019].

[11] D. G. M. Jr., "'Smart Thermometers' Track Flu Season in Real Time," The New York Times, 16 January 2018. [Online]. Available: https://www.nytimes.com/2018/01/16/health/smart-thermometers-flu.html?module=inline. [Accessed 5 March 2019].

[12] S. Maheshwari, "This Thermometer Tells Your Temperature, Then Tells Firms Where to Advertise," The New York Times, 23 October 2018. [Online]. Available: https://www.nytimes.com/2018/10/23/business/media/fever-advertisements-medicine-clorox.html. [Accessed 5 March 2019].

[13] N. Mancall-Bitel, "The 'smart' baby technology raising today's children," BBC, 29 November 2018. [Online]. Available: http://www.bbc.com/capital/story/20181128-the-smart-baby-technology-raising-todays-children. [Accessed 5 March 2019].

[14] Internet Association, [Online]. Available: https://internetassociation.org/. [Accessed 7 March 2019].

[15] Industrial Internet Consortium, [Online]. Available: https://www.iiconsortium.org/. [Accessed 7 March 2019].

[16] J. Doward and A. Gibbs, "Did Cambridge Analytica influence the Brexit vote and the US election?," The Guardian, 4 March 2017. [Online]. Available: https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridge-analytica-what-role-brexit-trump. [Accessed 5 March 2019].

[17] N. Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far," The New York Times, 4 April 2018. [Online]. Available: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. [Accessed 5 March 2019].

[18] N. Feamster, "Announcing IoT Inspector: Studying Smart Home IoT Device Behavior," Freedom To Tinker, 23 April 2018. [Online]. Available: https://freedom-to-tinker.com/2018/04/23/announcing-iot-inspector-a-tool-to-study-smart-home-iot-device-behavior/. [Accessed 5 March 2019].

[19] E. P. I. Center, "Internet of Things (IoT)," Electronic Privacy Information Center, [Online]. Available: https://epic.org/privacy/internet/iot/. [Accessed 5 March 2019].

[20] N. Gibbs and L. Grossman, "Here's the Full Transcript of TIME's Interview With Apple CEO Tim Cook," Time, 17 March 2016. [Online]. Available: http://time.com/4261796/tim-cook-transcript/. [Accessed 5 March 2019].

[21] M. U. IOTAP, "IoT, Security and Privacy," Medium, 14 June 2016. [Online]. Available: https://medium.com/@iotap/internet-of-things-security-and-privacy-78bc0a41881b. [Accessed 6 March 2019].

[22] M. U. IOTAP, "On Privacy and Security in Smart Homes," Medium, 14 June 2016. [Online]. Available: https://medium.com/@iotap/on-privacy-and-security-in-smart-homes-543f62aa9917. [Accessed 6 March 2019].

[23] C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," IEEE, 7 July 2017. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7971869. [Accessed 10 March 2019].

[24] T. Economist, "Data workers of the world, unite," The Economist Group Limited, 7 July 2018. [Online]. Available: https://www.economist.com/the-world-if/2018/07/07/data-workers-of-the-world-unite. [Accessed 11 March 2019].