**CATHOLIC UNIVERSITY OF ZIMBABWE**

**FACULTY OF COMMERCE**

**BUSINESS MANAGEMENT AND INFORMATION TECHNOLOGY** 

**NAME : KUDAKWASHE W. RUKUNI**

**REGISTRATION NUMBER : R142212**

**LECTURER : MR F MASIMBA**

**COURSE : EMERGING TECHNOLOGIES**

**CODE : IT405**

**Research Topic**

Internet of Things and its application in the security sector and loss control departments.

**INTRODUCTION**

The current level of security productivity in the world can be seen to increase due to the rapid development of the technology and increase in demand for internet of things devices. The main challenges being faced with companies have been tackled using Internet of Things solutions, and this could result to mitigating the level of demand for smart security internet of things solutions over the long run.

Although companies have met significant security challenges in the past, targeted increases in productivity have been set and achieved. However, in the next few decades to come these companies may realize losses due to the ongoing issues raised by lack of security. Some of these challenges include theft, vandalism, trespassing amongst others.

In this connected world where people computers and physical objects cooperate to solve complex tasks, a big amount of data and information is gathered. A very critical aspect would be to manage the knowledge so as to make the right decision. Smart security adopts a goal of the security sector where the assets combine both information technology and internet of things solutions. This combination allows for a more secure management of resources and knowledge so as to enhance asset value, reduce loss from damages or theft and increase profitability in a significant way.

With this in sight the protected assets become a substrate where different kinds of sensors could acquire much needed data. The sensors are then connected in a local network and linked to the Internet, such that any challenges faced in the security sector can be known of within a matter of seconds after it has happened. The real-time streaming data is then stored in complex database containing all the necessary knowledge about the attacker’s activities. Intelligent programs and mobile applications connected with the knowledge base run to make real-time decisions, sending acting messages and suggestions to the loss control and administration or to the domestic back-end systems as evidence and data for further research and development in the Artificial Intelligence field.

This term paper seeks to highlight on the use of internet of things concepts in the field of security amongst companies across the globe.

**BACKGROUND OF THE STUDY**

Despite the growing number of law enforcers, high demand for security officials in companies and also the high employment rate found in the security sector, there will always be a loop hole surrounding the protection of assets. To meet the interests of stakeholders and customer’s, companies will have to adopt new technologies so as to gain a much needed edge in protecting their assets.

New security applications in smart security adds precision through the use of internet of things, this will enable companies to increase operational efficiency, lower costs, reduce loss, and improve the quality of their produce.

Smart security represents the application of modern Information and Communication Technology (ICT) into the security sector of any company or firm. It can also be defined as a capital-intensive and hi-tech system development for protecting valuable assets that may serve the society.

In internet of things based smart security, is a system that is built for monitoring the company assets with the help of sensors (motion, sonar, fuel level, alarm or buzzers, face detection, to mention but a few) and automating the reporting system. The loss control or the security department of any organization, can monitor their company assets from anywhere around the globe. Internet of things based smart security is highly efficient when compared with the conventional approach. Hiring a security guard can prove to be a total waste of time as some end up sleeping on the job or else committing treason.

The applications of internet of things based smart security not only targets conventional, large protection operations, but could also be used to uplift other growing or common trends in technology like vehicle anti-theft systems and home security.

So this brought about a question of whether or not if internet of things devices can improve the quality of company stakeholders and customers, by increasing integrity, availability and security. In simple terms companies need to practice this so as to operate efficiently.

**CURRENT TRENDS**

Currently the internet of things industry is disconnected from device to device. Each internet of things device can only pass information to the internet and this information is stored within online databases. However, these devices lack the ability to share information and communicate with each other.

Devices are just things, for example, a smartphone, it knows its surroundings using cameras, thermostats, GPS modules amongst others. An internet of things device can be an anti-theft system device, with sensors that help in reporting an intrusion and also confirming the crime scene.

So now, for all internet of things devices to communicate on a major scale, that would be revolutionary as current trends have proved that these internet of things devices cannot communicate with each other. The sharing of knowledge that has to happen between these internet of things devices can prove to be very useful to our lives in the following few decades ahead.

The internet of things market revenue is $212 billion. An estimate of 20.4 billion internet of things devices have been recorded to be online in 2020. The number is expected to rise to 75 billion devices by the year 2025.

Internet of things devices are only providing problem solving techniques. They however still lack the ability to communicate with each other so as to create a more customized experience which is something the whole world is anticipating for. In a world where a wrist watch can wake you up every day at 7am and opens your curtains then switches on your coffee machine thus automating your daily morning routine.

Currently in the security sector, internet of things devices can only report a problem to a centralized database. This database cannot communicate with the smart security device hence creating a problem of miscommunication. If a false alarm had occurred, it is only when police have arrived that they discover it is a false alarm.

**FUTURE TRENDS**

What this Internet of Things project is aiming to do is to provide devices the ability to search, trade and share knowledge amongst each other. It aims to create an eco-structure with billions of devices that can communicate seamlessly, autonomously and securely. To achieve this, a system that consists 3 levels which are the intelligent block chain (this will ensure integrity, security and availability), an open economic framework (decentralized search systems or databases) and autonomous economic agents (the internet of things devices).

These networks are then installed in small areas so as to provide each device with knowledge and information on a shared medium source of information, hence automating the problem solving process. If it is a security device reporting an attack surrounding internet of things devices should be notified about the attack at real-time as well.

These internet of things devices will gather and process information from different sources, creating knowledge which delivers valuable insights that can make a meaningful impact to our lives. Today to organize a simple flight trip you need a multitude of applications to book services like taxis, flight and hotels. These internet of things devices will do it for you in the least amount of time, based on your preferences, thus taking the stress out of travel all together.

For example, these smart security devices that can be integrated into the security sector of companies. They can report an intrusion to maybe the nearest police station or the nearest officer to the crime scene, seamlessly, automatically and securely. Whenever an attack occurs to company assets the problem is solved before it has escalated to difficult heights.

It is assumed that by the year 2023, 70% of all new vehicles will be connected to the internet. This shall give a rise to self-driving vehicles, artificially intelligent vehicles that can converse with their owners. This will prove to be revolutionary and change the world as a whole. Imagine a world where all the decisions are being done for you by your vehicle. It knows the shortest routes, it knows what food you prefer, it knows your speed limits and schedules. All we have to do is literally sit inside our cars and get to point B.

As we continue to develop in the internet of things security sector we can find out that there has not been anything said on the issue of hackers. Hackers seem to grow even wiser and more dangerous by the day. So if all these internet of things devices are still vulnerable in the few years to come, we will have a very big problem at our hands. Our own security as a company can turn its back on us. Hackers can lock us out our very own system and demand ransom.

It is now very evident, that smart security will be an area in which investment and research is of the necessity to deploy countermeasures. Smart security will be a growing trend in the next few years to come. As mentioned earlier we need to observe how the use of block chain technology could be a key figure to achieving higher security in the internet of things industry.

For example, a combination internet of things devices can be put in place whereby fences made of polymer-coat can sense an intruder before they even reach the target. These will communicate with the motion sensors and surveillance to keep them alert for any movement which might happen. When they sense motion they can communicate with alarms and other reporting features so as to notify a nearby automated neighborhood watch. This automated process will involve the devices collecting valuable information and processing data from an intrusion. Such that the camera will recognize the intruders faces using artificial intelligence and then they will identify the intruders by name and registration numbers. Hence this will create a very reliable form of smart security in the future.

The only problem that seems to have no solution in the internet of things security sector would be availability of human judgement since computers do not have human feeling. They can fail to take action where it is required urgently. For example, when a company asset is under attack the smart security device may succeed in reporting however they will fail to arrest the intruders. Unless the developers can integrate more devices that can automate trapping the intruders in a cage. But this is only still a theory that may be approached in the following years to come, since currently the internet of things field has not yet managed to allow for smart security devices to communicate.

From the above example we can learn that the need for these internet of things devices to communicate will be the turning point in the future of smart security. In my opinion, the future of internet of things in the security sector will be headed in a ditch pretty soon by until this happens it is the back bone of the prophesized “technology revolution”.

**CHALLENGES**

Internet of things devices lack encryption and decryption abilities. These devices are usually constrained and they cannot perform encryption and decryption. Therefore, this will affect the security features of the devices as they are vulnerable to hackers. Data breaching can end up causing a major upset whereby the hackers may demand a ransom after taking hostage of an internet of things device. For example, autonomous cars and vehicles deliberately crashing into buildings like the September 911 scenario.

The growing use of the smart devices will result in an increase of intimacy towards the devices by their users. When the user becomes too close to their smart device and begin to share their private data with these devices. The devices will definitely become vulnerable to data breaches and even accidental data sharing. This will affect the privacy issues that arise from using a shared medium source of data.

Internet of things devices lack human feeling. They do not feel remorse, anger, or even go out sad. These security sensors such as the motion sensor may not even know the difference between a human motion and an animal motion hence resulting into false reports.

These smart security device protecting company assets may report a natural intrusion. It could be an animal passing by or perhaps a fruit drop that might have caused the anti-theft system to report an intrusion to the nearest people and thus causing a lack of faith in these devices. People love the fact that they do not have to think in order to overcome a problem, people prefer having so much free time and if these devices fail to save them time then they are of no use to them.

There is a lack of compliance from device manufacturers whereby they do not provide updates and these device use weak and common passwords that are easily hackable. The encryption process on these devices is very poor and may lead to vulnerabilities. This will the overcome the whole point of calling smart security devices secure. The whole purpose is to make the devices secure enough so as to secure the company assets without any threats lurking.

The major challenges that are being faced in the smart security sector are lack of updates on sensor devices and also these devices lack of the ability to communicate with each other. In order to over these challenges the manufacturers need to invest more into Research and Development.

**DISCUSSION**

The general rule of thumb is set to state that assets need protection hence why we have security guards being employed. For valuable company assets they may need an anti-theft system. There’s a pool of reasons for preventing intrusion to company assets depending on the type of company asset and its purpose.

Sometimes the company assets are too expensive and may have sentimental value to the community such as prestigious car, company documents, generators, company premises, specific company offices also plant and machinery.

Sometimes the company asset is difficult or impossible to replace if lost or damaged. This can be due to a low production of these assets for example at ZESA, they have a very limited supply of transformers since they have to import them from other countries

Also company assets and product may be at risk from intruders because they are easy to acquire and steal. For example, food items and office documents or stationery. In other scenarios the protected items may be left unattended in very unsafe environments for a certain amount of time hence becoming vulnerable to theft. Just like leaving laptops in the library or place of work. The need for surveillance is necessary so as to protect the employees.

In other cases, improper use of the item may cause considerable damage or encourage further unauthorized actions. The assets are then closely monitored to see why they are being damaged frequently. Another reason will be that the protected item would be desirable to others such as jewelry.

Sometimes the protected asset is otherwise unobtainable for example alcohol and tobacco products. Once an intruder opens a bottle of alcohol the company cannot put the bottle back on the shelf thus leading to loss. Now when a smart security device is in place it should act very fast before the alcohol bottle is opened. This analogy works best in smart security for supermarkets and shops. However, for company assets the damage may have been already done the moment an intruder steps on the scene.

Smart security systems have evolved to counter new theft techniques as they have appeared in the society. The choice for a particular anti-theft system is dependent on the factors mentioned below.

Financial cost of the asset, in addition to the initial capital cost of an asset, the cost of replacement or recovery from theft of the asset is usually considered when considering the cost of installing an anti-theft system. This cost estimation usually determines the need for securing it. More expensive assets will generally be secured with a higher cost anti-theft system, while low-cost items will generally be secured at a lower cost anti-theft system.

Threshold for theft. As we know smart security devices are designed to raise the difficulty of theft to an infeasible level. The kind of system implemented often depends on the acceptable threshold for theft. For example, keeping money in an inside shirt pocket increases the difficulty of theft to occur. threshold of theft is often dependent on the environment. Usually in suburbs theft is very unlikely to occur more than in the ghetto. Once the magnitude of something to occur is high then there is need for prevention.

Ease of use of smart security devices. The average anti-theft device does not require any additional effort while using the device. In practice, users of security systems may intentionally reduce the effectiveness of an anti-theft system to increase its usability. The more user friendly a smart security device is the more effective it is for the user.

So with all this in mind we can now speak of methods of prevention using these smart security devices. There are a lot of prevention methods which include preventing removal of assets, raising the awareness of theft within the area, security tags, tracking software and also disabling the assets once removed such that they become unusable. All these methods will reduce the need for theft of company assets. Once an intruder knows about this then they will not attempt stealing the asset.

In a nutshell the major talking point of smart security revolve around the fact that companies need protection for their assets so as to avoid unnecessary expenditure.

**CONCLUSION**

To conclude this term paper I will highlight on an Internet of Things device that I am currently working on. This “thing” is a smart security device designed to work as an anti-theft device for companies that struggle with care and protection for their valuable assets.

For example, ZESA, they have neglected their transformers for a very long time now. The community always seems to complain that the electricity faults that result from transformer attacks by intruders usually take months to get fixed. If ZESA realizes that their assets are valuable and should not be tempered with they need to avoid transformer theft and vandalism. The best way to avoid this would be to employ the smart security device that I am currently working.

The device consists of a motion sensor, to detect nearby movement. It also includes a camera and a very bright led light so as to capture clear photos of the intruder. Then lastly it consists of a buzzer alarm that will scare the intruder away. It would be very nice to integrate an Arduino Uno with Wi-Fi so as to upload images directly on to the Internet. Currently the device can only upload data via serial communications to the local server running on xampp.

In future this smart security device will be able to communicate with other nearby devices such that when the device reports an intrusion, nearby devices can be notified and they in turn notify authority thus swift action can take place. Also this smart security device should be able to store data about these breaches hence highlighting areas of threat more accurately thus preventing further damages.

The future for smart security is honestly quite bright, however this is only until something is done about how these sensor devices can be made secure enough to resist hacking and penetration. As mentioned earlier in this term paper, the internet of things industry need to put in place a system that consists of 3 levels. The block chain level, a secure decentralized database level and the autonomous smart security devices level.

So in conclusion this is how internet of things has been applied in the security sector for companies. The companies use smart security devices to protect their assets and this allows for stakeholder and customer satisfaction.

**RECOMMENDATIONS**

According to my opinion companies need to invest more in protecting their assets. This approach will definitely increase shareholder, stakeholder and customer satisfaction. The researcher here has realized that once company assets are damaged the above mentioned parties will suffer the most. The best way to avoid bankruptcy and losing favor from the above mentioned parties would be to protect their investment.

This research was done with an aim to increase satisfaction. Sometimes when these intrusions occur the affected parties will grieve hence this may result to a lot of negative factors such as employee turnover and denial of service. In the case of ZESA, a manager might get fired for not protecting company assets. Also customers may go for months without electricity even though they would have paid for the service.

The features that were implemented are listed below:

Administrator rights

a. View intrusions on local server.

b. Refresh database view.

Customer rights

a. Report a fault.

b. Register a new customer account.

c. View a history of reported faults by the customer.

I recommend this idea of employing smart security devices into companies so as to avoid any inconveniences that may rise due to intrusion. The ant-theft devices will protect the company investments.

**REFERENCE LISTS**

Internet of things – Wikipedia.

5 eyes statement of intent regarding the security of the Internet of Things (July 2019).

AT&T: The CEO’s Guide to Securing the Internet of Things.

Australia Draft Code of Practice – Securing the Internet of Things for Consumers.

Alliance for Internet of Things Innovation (AIOTI) – Report on Workshop on Security and Privacy in the Hyper-Connected World.

Atlantic Council Scowcroft Centre for Strategy and Security – Smart Homes and the Internet of Things (issue brief).

Department of Homeland Security – Strategic Principles for Securing the Internet of Thing.

IoT Security Foundation: IoT security training: <https://www.iotsecurityfoundation.org/iot-security-training>.

European Union Agency for Network and Information Security (ENISA) – Baseline Security Recommendations for Internet of Things.

Internet of things trends 2020 – YouTube.

Microsoft: Internet of Things security best practices <https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-best-practices>.

[GDPR] Article 29 Data Protection Working Party – Opinion 8/2014 on the on Recent Developments on the Internet of Things

Cloud Security Alliance – Future-proofing the connected world: 13 steps to Developing Secure IoT Products.

Internet Engineering Task Force (IETF) – Best Current Practices for Securing Internet of Things (IoT) Devices: <https://tools.ietf.org/html/draft-moore-iot-security-bcp-01>.