IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 5)
Available online at: www.ijariit.com

An introduction to context-aware security and User Entity Behavior Analytics

Yash Arohan
yash.arohan@gmail.com
Thakur College of Engineering and Technology, Mumbai, Maharashtra

Ashwin Yadav
ashwindyadav198@gmail.com
Thakur College of Engineering and Technology, Mumbai, Maharashtra

Aakash Pandey
aakashpande201@gmail.com
Thakur College of Engineering and Technology, Mumbai, Maharashtra

Shardul Churi
churishardul@gmail.com
Thakur College of Engineering and Technology, Mumbai, Maharashtra

Manvi Saxena
saxena.manvi11@gmail.com
Thakur College of Engineering and Technology, Mumbai, Maharashtra

Akshit Vaghani
akshit.vaghani7@gmail.com
Thakur College of Engineering and Technology, Mumbai, Maharashtra

ABSTRACT

A context aware system is recognized as a "system which uses any context information previous to, or in the duration of, service stipulations", whereas the main goal of this system is to identify any suspicious activity done by the users. The mobility feature of most computing and personal devices has made the 'context of the user' an important aspect of the system. Nowadays with the ever-increasing digitization of the workplace, employees are using their personal devices along with the organization resources provided to them. Context Aware security systems vary from conventional systems, as they provide unique characteristics such as name, geolocation, time of day or type of endpoint system to boost information security decisions. Combine this with a model that notifies and alienates any abnormal activity by the user, we have a strong security measure against harmful cyber activities such as unauthorized end users accessing confidential data, preventing users to download sensitive data onto external devices, and so on. Context-aware security systems address the usability challenge of accessibility and authentication, i.e., to use inferential information such as geolocation, identity, type of endpoint device, or time of day to enhance information security decisions. The use and importance of this system is increasing and therefore plays a huge role in prospective pervasive systems. The goal of this paper is to introduce the reader to the concept of context aware security and lay the groundwork that one needs to get accustomed to the topic, by extracting various topics from different research papers.

Keywords— *Authentication, Context-aware application, Context-aware Security, User Entity Behavior Analytics.*

1. INTRODUCTION

Ever wondered a scenario where you could give your users all the access they need, without the worry of attackers being able to obtain valid user credentials and using it for their own personal good!

Usually, security is simplified by basing it on a series of yes or no decisions whenever the user logs in. But, what if you can structure the same security decisions on the who, what, where, when and why behind the user requests, you can significantly lower the chances of giving access to an attacker with valid credentials without hindering the users from doing their work. [17]

Practically though, security has been a static process of administrators saying “no” and denying access to users and preventing them from easy access to the resources that they need to get their job completed. This “static security” slows down user productivity and the overall work of the organization.

To be fair safeguarding user credentials from vulnerability is quiet an impossible task. Massive amounts of credentials uncovered in data breaches are circulating online, and every fortnight million more keep getting exposed, either through weak servers or through intrusive acts. Add to the fact that users keep getting fooled by ever convincing phishing attacks to voluntarily give up their credentials, the plans for identity and access control go for a toss.

These intrusions can lead to many business-destroying thefts and much more damaging acts of cyber-terrorism. Thus, we need to implement a better approach. With the increase in the number of mobile users and the increasing sophistication of attacks, context-aware security can be our way to fight such intrusions and data breaches as it can give a real-time evaluation of the “who, what, when, why and where” surrounding each request for resource or network access [13].

Context aware security (CAS) can be defined as - “*the use of supplemental information to improve security decisions at the time they are made, resulting in more accurate security* *decisions capable of supporting dynamic business and IT environments. The most commonly cited context information types are environmental (such as location and time)".* [12]

How context-aware security is different from traditional security?

Context Aware Systems are different from traditional systems as they provide unique features such as heterogeneity, high complexity and artificial intelligence. The disadvantage of static IT security is that it has a very limited view of each request for access. When the organization accepts or rejects access based on a string of yes or no decisions, the result is likely to be one that denies access to too many users with legitimate needs. But with context-aware security, the reason for the user's need to access can be analyzed by considering various different factors and thus increase the ease to legitimate access. Context-aware security thus helps organizations to safely create a passage of access to legitimate users based on real-time decisions on the risk associated with the various aspects of security information.

Moreover, increased computation has made it easy for script kiddies to crack password control, making Single Sign-on (SSO) a poor authentication technique, unless the password is 9-12 alphanumeric characters long, because the password is all that the attacker wants to hijack your account. It is often recommended by many security researchers that using a Multi Factor Authentication (MFA) is the best way to protect your online identity, but to what extent? If an attacker intends to intrude a user's privacy, he or she will do so with enough time and research to bypass MFA, so it cannot be called foolproof. So how else can a system authenticate that they are the real person and not someone imitating them with the right credentials? Advances in machine learning and analytics have made it simple to analyze security data and identify standard behavior profiles for users or computer systems. This makes it easier to detect behavioural patterns that could be an attacker's malicious operation.

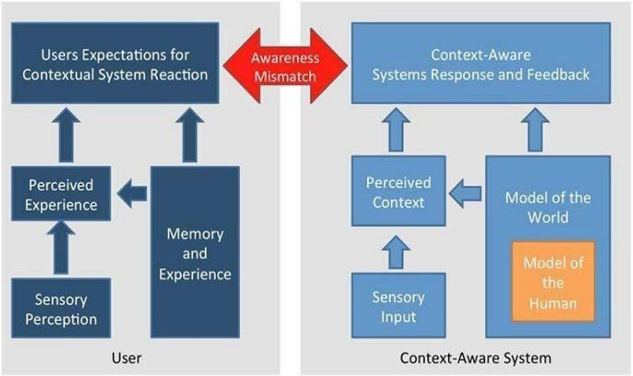


Fig. 1: Context - Aware System

The Context-aware security is a configurable algorithm to weigh the additional adaptive questions according to the organization's needs, user populations, threats, practices, applications and infrastructure. The algorithm returns scores to control points (such as access management tools, firewalls and encryption technologies) that allow or deny access or enable step-up (two-factor) authentication prior to authorizing access- a principle called adaptive authentication.

The '*Snowden disclosures*' can be seen as a perfect example as to how context-aware security could have saved the organization from such a data breach. Snowden was able to point out the flaws that the static security infrastructure had. It is said that Edward Snowden logged into the NSA networks during non-operational hours for the officially approved project of constructing a disaster prevention system for Booz Allen Hamilton under an NSA contract. The fact that he was logging in to the system after work-hours may or may not be considered erratic considering his job. However, it is also said that he borrowed around twenty to twenty-five passwords from his colleagues and managed to achieve root level privilege. He then went on to download around 1.7 million files from the network onto a USB stick. It's said that downloading such a massive number of files to a USB stick is rather unusual behavior for a person working on a disaster prevention system.

If context-aware security was used as the base of cyber security, Snowden may or may not have been flagged due to his after work-hour login. But his action of copying such a large amount of data to an external source, that too in Hawaii, would have been considered as an abnormal activity on his part and it would have been subsequently flagged. He probably would have been flagged for acquiring super root level privileges at the NSA Headquarters in Maryland. Abnormal usage of 25 peer accounts all associated to Snowden's IP address would have almost definitely set off alarms had the appropriate security measures been implemented. [16]

2. CONTEXT AWARE REQUIREMENTS & DESIGN CONSIDERATIONS

Before diving deep into the discussion regarding how context-aware can be used to deal with various potential security issues, a brief insight into the basic categories of "context" will be thrown on to the categories of context as a whole. Most of the studies have been published with various categories of context. However, majority have agreed collectively upon three - four as the major ones. For instance, in a research conducted by Chen and Kotz, four basic categories of context have been mentioned. These are: Computing Context, User Context, Physical Context and Time Context. A brief description about the information and areas covered by each is given below:

- **Computing context:** includes areas and knowledge related to device access, inter-networking, and other computer related assets such as printers and workstations, CPUs, memory resources, etc. Another significant feature and characteristic of context-conscious applications in the context of computing is that users often use several devices [3]. Therefore, they prefer tools that have the facility to perform several functions at the same time, such types of apps include smartphones and Personal digital assistants, etc.
- **User context:** contains information related to the user's use of the application that includes the user's personal information, preferences, current location, potential activity, and so on. The choice of users can be defined by the specifics of the type of preferences they have. For example, some users are willing to go to some particular location by taxi or hire private transport, while some other users are willing to go within walking distance. Therefore, for this purpose, a storage portion or facility is needed, and the use of preference related information is effective.
- **Physical context:** It covers areas and offers information on location, time, destinations, weather, physical, environmental conditions, and so on. For example, in most cases, users need access to information such as weather forecasts, route directions, current traffic situations, and temperature-based updates. Therefore, these kinds of useful requirements need to be revised on a regular basis and also be made available to the users.

- **Time context:** provides details and links to time and calendar details on a regular, weekly or monthly basis.

3. FACTORS TO BE CONSIDERED WHILE CREATING A CONTEXT-AWARE SECURITY SYSTEM

To create a successful context aware system, one has to ensure sufficient factors are considered so as to maximize the attention to details while minimizing employee privacy intrusion. Currently context aware security systems are based on utilizing the following factors:

1. **Bio-printing:** By using the bio-printing technique we can analyze how hard and fast users type, what are their habits and how they use the mouse. For example – if an employee's typing is slow and suddenly at 3 AM (which is not the usual office hours) someone is typing from the same device at a different rate then we can know that this is not the same user and the risk score increases.
2. **Location Tracking:** Location is a very important indicator of behaviour. Basically, we can detect whether any request is originating from a peculiar location or not. Example – if an employee requests access to the system from a hotel room, then his risk score increases. Also, access initiated from specific geographic locations which are known to aid malicious activity can be prevented.
3. **Behavioural Profiles:** Nowadays, companies maintain profiles of users, clients, accounts and even peer groups wherein they store data related to a person's habits. They monitor how the behaviour changes from month to month or device to device. By comparing the user's real time behaviour with the past behaviour, the company analyses whether there is a security concern or not. Also, two lists can be maintained, that is, a blacklist and a whitelist. People in the blacklist are prohibited to request access and whitelist people are authorized to request for access. These lists are made from a list of forbidden or approved networks or network addresses. Moreover, historical analysis of any browser use that falls outside the normal behaviour of the user can be also considered. For example – even if a company's new developer is poking around the network from his desk, on his laptop, during the working hours, on-premises he will still be denied access as his account name and role do not match.
4. **Third party big data***:* Big data security is a collective term for all measures and tools used to protect both data and analytical processes from attacks, thefts or other malicious activities which could be harmful or averse to them. Essentially what makes data big is that, we have far more ways than ever before to gather information from far more sources. Think of all the billions of devices that are now enabled by the internet-smartphones and sensors on the Internet of Things which are just two of the many [15]. Now think about all the big data security issues that could be developed! For example – say a criminal is setting up a fake clinic with fake doctors in order to get their hands on patient insurance IDs and bills for sham procedures. Big data analytics can alert companies to the fact that these so-called clinics are located in remote office malls with low population.
5. **External threat intelligence:** *"Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and action-oriented advice about an existing or emerging menace or hazard to assets. This intelligence can be used to inform decisions regarding the subject's response to that menace or hazard." — Gartner.*
   - **External Sources:** External sources can be very diverse, with several degrees of trustworthiness. "Open Source" information (i.e. security researchers, vendor forums, and publicly accessible reputations and block lists) can provide markers for identification and context. Private or commercial sources of threat intelligence can include threat intelligence feeds, structured data reports (such as STIX), unstructured reports (such as PDF and Word documents), emails from sharing groups, and so on.
   - **Internal Sources:** Your own network reveals which information is genuinely important to your organization. When using threat response data from your own network (i.e. log files, warnings, and incident response reports) you can identify and avoid attacks. If you use a Security Information and Event Management(SIEM), this is a great place to start. SIEM already includes several primary sources of internal network event data such as event logs, DNS, firewall logs, and so on. For example - are contractors and competitors being targeted? Are certain accounts associated with fraud? Are malicious attackers using the same IP blocks across multiple attacks?
6. **Time:** It identifies any unusual access requests made by the user outside of normal times and days. For example – if an employee works after his or her working hours then their risk score increases. Your own network shows which knowledge is genuinely important to your organization. You can identify and avoid attacks when using threat data from your own network (i.e. log files, warnings, and incident response reports).

4. MODELS

In a scenario where there are numerous parameters to be considered, there arises a vast array of possibilities that need to be computed. Along with these possibilities, we need to calculate the probability of them occurring. Simple algorithms do not possess the capability of computing these probabilities. To handle this, we can make use of certain machine learning tools; Models like Markov Chain, Naïve Bayes, Decision Tree, and so on, which are better at handling probabilistic analysis, can be used to perform this task.

4.1 Markov Model

A Markov Chain-based detection model [2] can be described as a discrete-time stochastic process which denotes a set of random variables and defines how these variables change over time. Markov Chain can be applied to illustrate a series of events where, what state will occur next depends only on the previous state. A series of events represents user activity and state represents sensor conditions (i.e., sensor values, on/off status) of the sensors in a smart device. We can represent the probabilistic condition of the Markov Chain as in Equation 1 where Xt denotes the state at time t.

$$P(Xt+1 = x \mid X1 = x1, X2 = x2, \dots, Xt = xt) \\ = P(Xt+1 = x \mid Xt = xt)$$

Equation (1)

when,

$$P(X1 = x1, X2 = x2, \dots, Xt = xt) > 0$$

We use a reformed version of the general Markov Chain. Here, instead of predicting the next state, we determine the probability of a transition occurring between two states at a given time. We determine conditions of sensors for time t and t+1. Let us assume, *a* and *b* are a sensor's state in time t and t+1. We look up for the probability of transition from state a to b. If transition from state a to b is nefarious, the calculated probability from transition matrix will be zero. For example, consider a geolocation 40°41'44.7"N 73°55'02.8"W which corresponds to a place in Brooklyn, New York. A transition to a geolocation 40°42'00.5"N 73°54'58.7"W would be reasonable and wouldn't cause an alert. However, a jump to a geolocation 55°45'55.4"N 37°38'17.0"E corresponding to Moscow, is extremely unlikely and would indicate the use of a location spoofing tool, raising an alert.

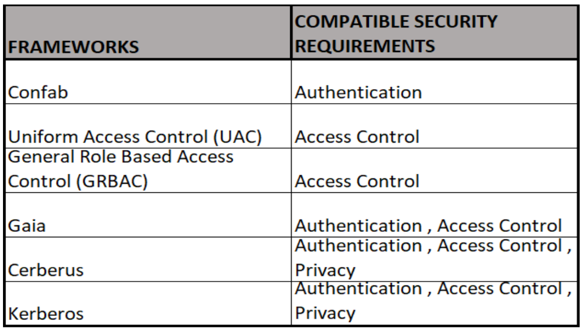
Naïve Bayes:

Naïve Bayes model [2] is a simple probability estimation method which is based on Bayes' method. The main assumption of the Naïve Bayes detection is that the presence of a particular sensor condition in a task or activity has no influence over the presence of any other feature on that particular event. The probability of each event can be calculated by observing the presence of a set of specific features. We consider users' activity as a combination of *n* number of sensors. Assume X is a set which represents current conditions of *n* number of sensors. We consider that conditions of sensors are conditionally independent, which means a change in one sensor's working condition (i.e., on/off states) has no effect over a change in another sensor's working condition. The probability of executing a task depends on the conditions of a specific set of sensors. So, in summary, although one sensors' condition does not control another sensor's condition, overall the probability of executing a specific task depends on all the sensors' conditions. As an example, if a person is walking with his smartphone in his hand, the motion sensors ([6] accelerometer and gyroscope) will change. However, this change will not force the light sensor or the proximity sensor to change its condition. Thus, sensors in a smartphone change their conditions independently, but execute a task together. We can have a generalized model for this context-aware detection as follows:

$$P(X \mid c) = \prod_{i=1}^{n} \quad P(X_i \mid c)$$

5. FRAMEWORKS

Previous studies have proposed various frameworks for implementing efficient and effective security on user's information in the context and the context-aware system as a whole. The main purpose of implementing these frameworks is to gain and acquire various security related requirements and models which were mentioned before. However, each framework has come up with its own purpose of implementing and serving with a unique kind of security requirements and models. For this reason, each separate framework has got its importance and is therefore definitely required to be implemented and fulfilled. The following are brief details about various frameworks that have been used to implement various security requirements along with the kind of unique purpose they fulfill and which is therefore being used in the context-aware systems.



FRAMEWORKS	COMPATIBLE SECURITY REQUIREMENTS
Confab	Authentication
Uniform Access Control (UAC)	Access Control
General Role Based Access Control (GRBAC)	Access Control
Gaia	Authentication , Access Control
Cerberus	Authentication , Access Control , Privacy
Kerberos	Authentication , Access Control , Privacy

Fig. 2: Basic Context - Aware frameworks

- **Confab Framework:** Confab framework is fundamentally designed to provide safety and reliable security for information relating to the position of users in ubiquitous systems. In addition, its working hierarchy is focused on some basic research, relevant to the privacy criteria of end-users and application developers. The user's private information is collected, stored and then handled on the computer of the user instead of being stored on another computer for security purposes.
- **Uniform Access Control (UAC):** Covington *et al.* [10] is a control framework specifically designed for environmental roles. In addition, it was announced and asserted as a further expansion of the Role-Based Access Control (RBAC) model. Moreover, it is responsible for evaluating and assessing security issues relevant to context-aware systems and applications in ubiquitous environments.
- **General Role Based Access Control (GRBAC):** Certain functions in the system are based on another structure called the General Role Based Access Control. Generally, the RBAC framework is a basic model that only covers and relates to a subject-oriented approach, while the GRBAC allows for the definition of access control policy, depending not only on the subject but also on other key and important factors such as the object or the environment.
- **Gaia:** This is planned to assist in the development of smart space applications such as smart homes and meeting rooms. It consists of a collection of core resources and a system for the creation of distributed context-aware applications [1]. Gaia's remaining four services support various forms of context-awareness, and include the following:
    - **Context service:** This helps applications to find providers for the context details they need.
    - **Presence service:** tracks individuals entering and leaving a smart space (including people as well as hardware and software components).
    - **Space repository:** maintains details of hardware and software components.
    - **Context file system:** It combines files with specific context information and dynamically creates virtual directory hierarchies based on the current context. Its main purpose, therefore, is to grant permission or access to authentic and actual users to use the system facilities.
- **Cerberus & Kerberos:** Other frameworks such as Cerberus & Kerberos are basically used to meet and implement the various security requirements in the context-aware systems and applications such as identification, authentication and access control. Nevertheless, Cerberus is a mechanism for which the emphasis is on the authentication and confirmation of the identity of the individual seeking access to the resources and benefits of context-aware systems.

- **Preferred Framework:** Nonetheless, Kerberos, along with the Cerberus architecture, is highly superior to the other architecture, since they focus on verifying and validating the identity of the user requesting access to the services and benefits of context-aware systems. This validation and verification can be done by making use of information and data related to the user's context, which includes fingerprint, voice and face recognition, etc.

• 6. APPLICATIONS

The context-aware computing can be used for various other applications because of the rise in technology nearing ubiquitous computing. Not just in the security space but also helping in personalizing user experience, which can be seen in [6]. Context-aware is useful in applications relating to fetching information, giving commands, ease of manual actions and automating some of these manual actions. Some of the known common real-world applications are:

a) **Smart - Home systems:** A lot of the applications in the Smart Homes are context-aware and based on the environment in which an access request is made, their behavior can be altered. For example:
   - Certain appliances can be accessed only if the request is made from a certain location or at a certain time.
   - In smart-intercom application permission to talk to a person in another room might depend on the activity the person is currently doing. Requests can also be triggered even though the resident has not explicitly made that request.
   - One potential application is allowing elderly citizens to remain in their home instead of moving to care-homes. If the person falls or injures themselves, the Smart Home system could detect the emergency and respond by requesting medical aid. This request will be automatically generated and approved based on the context of the incident. Other conditions such as time of the day, home temperature or the location from where the request is made are also considered.

b) **Context Aware Patient Monitoring:** The rapid worldwide growth in the senior population, chronic conditions and the costs associated with caring for them requires a new model for care and collaboration. Context- Aware system comprehensively evaluates this kind of knowledge and increases the quality of medical care. The application will aim to provide a standardized procedure for healthcare providers to use new sources of data from medical devices and sensors for smarter healthcare. So, the answer is the use of medical devices with sensors that are in-built to collect relevant data such as blood pressure, glucose level, weight, and automatically transmit these results to a personal health system and then eventually to the monitoring service. Thus, the nursing staff can keep a close track on the patient's health condition.

c) **Temperature Context-Aware Refrigerator:** This relates to a temperature-context-aware refrigerator and a method for controlling the same. The whole unit comprises of: an adaptive temperature sensor, sensing a temperature of at least one storage compartment, and when the difference between the sensed temperature and temperature set for the corresponding storage compartment is equal to or greater than a predetermined level, generating load-responsive operation information including a target temperature lower or higher than the set temperature; a temperature control unit for controlling a temperature sensor and the temperature context- awareness unit, and performing a load-responsive operation for controlling the temperature of the storage compartment by using the load-responsive operation information; and a database unit which is required for the temperature context-awareness unit to generate the load-responsive operation information.

But the most disruptive application of Context-aware is seen in the IT security space. The rise of Context aware security and user behavioural analytics has been accelerated by a simple realization - preventive measures are no longer enough to keep the corporate systems secure. Attackers will eventually invade your systems, and it's imperative to snuff them out as soon as they attack. The value of CAS, then, is not that it blocks any attackers or insiders from gaining control of critical systems. Instead, CAS systems can promptly identify when this has occurred, and alert you to the risk. Some of security related applications of CAS are as follows:

a) **Executive Assets Monitoring:** Hundreds of millions of dollars are stolen each year via wire transfers, usually through various mail frauds that trick the company executives into approving fraudulent transfers. Gaining access to computing assets of various executives may give attackers inside information related to earnings, profits, mergers, etc. An effective context aware system can automatically recognize behavior patterns and create a user model so as to monitor the system for any unusual access and usage.

b) **Insider Access Abuse:** Insider threat detection is challenging because no alerts are generated due to the behaviour being "trusted". By analyzing user behavioural patterns we can detect when a user is performing risky activities that are outside of their normal routine Many of these include detecting logins at strange hours, at unexpected frequencies, or accessing uncommon data or systems; modifying or increasing sensitive device privileges; correlating network traffic with threat intelligence to discover malware that interacts with foreign attackers; and finding data exfiltration.

c) **Data Exfiltration Detection:** Data exfiltration happens when confidential data is transferred illicitly to any outside mean. If the attacker transfers data over the internet, or copies it to another physical device, an alert can be raised on such an abnormal movement of data. The security system tracks enormous volumes of network traffic over protocols and compare the data movement to a user's or computer 's historical normal data transfer.

d) **Security Alert Investigation:** Security alert investigation by using legacy security tools, is a resource consuming process. Alerts usually consist of complex data in raw log files that can be understood by a bunch of experienced security analysts. Alerts generated may indicate an immediate response, but the inspection itself requires manual correlation of different log files, understand the meaning, manually selecting more and more data sources for hints and spending a substantial amount of time trying to determine the cause of the alert. CAS can considerably enhance the productivity of analysts in combination with a modern security solution. It offers better interface using machine-built timelines, allowing even someone like a junior analyst to go threat hunting.

e) **Lateral Movement Detection:** The method of lateral movement requires moving through a network systematically in search of sensitive data and resources. Probably the attack is initiated by misusing a low level employee's credentials. Once access is gained, other assets are searched by the attacker for weaknesses with the purpose of switching accounts, machines and IP addresses. The attacker then has a real opportunity to cause some damage when he gains access to administrative privileges. Lateral movement is quite challenging to detect by legacy security tools because the attack is scattered across the network, distributed among different credentials, IP addresses and machines. These independent events all appear to be ordinary. The User Entity Behaviour Analytics (UEBA) solution utilizes behavioural analysis to connect these "unrelated" activities and prevents these attacks before any damage occurs.

f) **Service Account Misuse***:* A service account is a user account that is expressly created to provide a security background for services running on the operating system of a computer. The security background defines the capacity of the company to access the local infrastructure and networks. Since server accounts have high privileges, the notion of such limited visibility seems bizarre. Any attacker who can make his way to such an account will have his work cut out. Thus, the service account misuse is a valuable use case for context aware security. By employing behavioural analytic capabilities, the system will automatically identify service accounts and flag any abnormal behaviour within them. [18]

7. PRIVACY ISSUES

Any digital experience that offers a more personalized and safe experience usually requires a privacy trade-off. Developments in Context-Aware Security & User Behavioral and Entity Analytics (UBEA) technologies offer a remarkable opportunity to enhance security by improving the effectiveness of both access controls and detective security [11]. They do this by analyzing additional data, contextual and behavioral, involving systems, apps, technologies, devices, and networks for business use.

Privacy concerns, which are related to current context aware systems, is a challenging issue. However, it has been discussed and mentioned by the researchers that there are many factors, which play quite a big role in raising some considerable privacy concerns and potential security issues in the mind of the user who is utilizing and accessing the context aware based applications. Some of the factors are:

- **Information Receiver reliability:** One of the factors which raises some privacy concerns among the users of context aware system applications is the reliability and truthfulness of the receiver who receives the user’s information. Users sometimes have an ambiguity or doubt on the credibility of the person who receives and uses their information. Hence, the only option left for the user, is to display confidence and trust on the authenticity and credibility of the information of the receiver.
- **Possible usage of user’s information:** Another factor mentioned by some researchers, which raises privacy concerns among the user, is the kind of usage, which is going to be made related to their private and sensitive data at the receiver’s end. The concerns arise when the users think or become doubtful about the proper or positive usage of their sensitive information.
- **Level of sensitivity in terms of users’ data:** According to studies, sometimes the level or extent of sensitivity and privacy of user’s data also raises a concern in the user’s mind whether to share or transmit this kind of data or not [2]. The user thinks twice whether it will be secure and good enough to make the sensitive data available and accessible to a third party or not.
- **Environment in which the user's information is shared or its privacy is being disclosed:** This is a factor, which raises concern in the user’s mind whether they should be sharing, and giving access to their information in various contexts and environments. Often the users are hesitant to disclose their information in any context or atmosphere because of questions about the context 's reliability and authenticity. Furthermore, a change or any update in the context also triggers some serious privacy concerns among the users and therefore prevents them further in sharing their sensitive and highly secure information in that very context.

8. RELATED WORKS

Works had started in context-aware security even before context-aware came into light with a general conception of improving security and diminishing user’s friction. Keystroke is a popular behavioural biometric. [3] Presented a survey on the large body of literature on authentication with keystroke dynamics. Researchers also suggested authentication token-based mechanisms to establish true users, e.g., wireless token [4].

There are certain approaches, which make use of touch behavior as biometrics for the purpose of authentication. [5] Proposes a password application, by which the user draws a stroke on the touch screen as an input password. Pressure, coordinates, size, speed and time of the stroke are used to identify valid users. Overall accuracy of this work is 77% with a 19% FRR and 21% FAR. Uses four features namely, acceleration, pressure, size, and time to distinguish between the true owner and impostor to increase the security of passcode. Its identification system achieves 3.65% EER. The user taps several times on a touchscreen with their fingers to enter a password.

It is the latest framework for Android which allows other researchers to improve implicit authentication schemes. Recently, there is some work addressing the user identification with behavior biometrics in a continuous or implicit manner. In those work, identification services run in the background and identify the current user in real time. For example, [6] continuously authenticates users based on 30 behavioural features, including touch features and motion sensor features. In this work, the EER is approximately 13% with a single stroke and converges to a range between 2% and 3% with 11 to 12 strokes.

SenGuard [7] combines motion, voice, location history and multi-touch data to identify users of smartphones, whose average error rate is 3.6%.

FAST [8] uses a special digital sensor glove to achieve highly accurate continuous identification. [9] distinguishes different users based on their gait, and the rhythmical body movements of human beings as they walk. Those works use special devices or motion sensors to enrich the identification features to improve the poor accuracy with pure touch information, but they ignore the scenario that the user uses a mobile phone while in motion.

9. CONCLUSION AND FUTURE MARKET GROWTH

Another promising future study is to employ the theoretical and conceptual notions of this research for developing real-world solutions [14].

Ever since the market of context-aware computing was valued at USD 42.21 billion in 2019, it has relied upon to arrive at an estimate of USD 200.04 billion by 2025, at a compounded annual growth of 29.9% over 2020-2025. With the continuous evolution in ubiquitous computing, context-aware computing has also seen a rise in demand in the computer science paradigm where computing can be made available at anytime and anywhere (due to the third wave of computing becoming popular over desktop computing in the last two decades).

Thus, this paper intends to cover all major points of context-aware computing which creates further new options to optimize security by analyzing overall context and decision making, based on the grand scheme. We hope that the proposed study will entice readers interested in context-aware studies like students and researchers, new to this field, who wish to understand the preliminaries, to become familiar with the various approaches and research efforts that have been made so far, and to realize the potential avenues for future; or method developers who wish to enrich their analysis by incorporating context information in existing or new algorithms; or application experts and tool makers who wish to design and manufacture novel context-aware systems for different movement applications. Context-aware services tend to be application dependent; however, the more generic the system, the more multi-user it will become.

Nevertheless, the primary challenges to developing a context-aware system can be summarized in recognizing unpredictable behavior, the automated collection of multi-resolution context information, the identification of variables that should be manipulated, quality assessment of the imported information into the system, handling the complexity of entities' interaction with the system, sharing context, and security and privacy issues. Looking into the future, each of the above challenges can be thoroughly investigated in a separate study.

10. REFERENCES

[1] Saad Almutairi, Hamza Aldabbas, and Ala Abu-Samaha, "Review on the Security Related Issues in Context Aware System", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 3, June 2012

[2] Amit Kumar Sikder, Hidayet Aksu, A. Selcuk Uluagac, "6thSense:user A Context-aware Sensor-based Attack Detector for Smart Devices", the 26th USENIX Security Symposium

[3] R. Joyce and G. Gupta, "Identity authentication based on keystroke latencies," Communications of the ACM, 1990.

[4] A. J. Nicholson, M. D. Corner, and B. D. Noble, "Mobile device security using transient authentication," IEEE TMC, vol. 5, no. 11, pp. 1489– 1502, 2006

[5] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and i know it's you!: implicit authentication based on touch screen patterns," in ACM CHI, 2012, pp. 987–996

[6] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," IEEE TIFS, 2013.

[7] W. Shi, J. Yang, Y. Jiang, F. Yang, and Y. Xiong, "Senguard: Passive user identification on smartphones using multiple sensors," in IEEE WiMob, 2011, pp. 141–148.

[8] T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, "Continuous mobile authentication using touchscreen gestures," in IEEE HST, 2012, pp. 451–456.

[9] M. Boyle, A. Klausner, D. Starobinski, A. Trachtenberg, and H. Wu, "Poster: Gait-based smartphone user identification," in ACM MobiSys, 2011, pp. 395–396.

[10] Z. Z. Michael J. Covington PrahladFogla and M. Ahamad, A context-aware security architecture for emerging applications, in Proceedings of the Annual Computer Security Applications Conference (ACSAC), Las Vegas Nevada USA, 2002.

[11] https://www.linkedin.com/pulse/privacy-conundrum-context-aware-security-user-behaviour-guillaume-no%C3%A9/

[12] https://techbeacon.com/security/how-behavioral-analytics-helps-close-credentials-security-gap

[13] https://blogs.cisco.com/ciscoit/b-s-11162015-bringing-context-aware-security-to-applications

[14] https://www.researchandmarkets.com/reports/4591230/context-aware-computing-market-growth-trends

[15] https://www.cyberdegrees.org/resources/hot-technologies-cyber-security/

[16] https://threatpost.com/avoiding-data-breaches-with-context-aware-behavioral-analytics/109679/

[17] https://www.oneidentity.com/context-aware-security/

[18] https://www.exabeam.com/ueba/top-10-ueba-security-use-cases/